基于身份的电子文档域密钥分发算法及协议

闫玺玺[1,2]，马兆丰[1,2]，杨义先[1,2]，钮心忻[1,2]
(1. 北京邮电大学 信息安全中心，北京 100876；2. 北京国泰信安科技有限公司，北京 100086)

摘 要：为了实现电子文档安全管理环境中域间用户的通信安全，采用双线性对构造了一个适用于大数量、动态域组的基于身份的域密钥分发算法，该算法实现了域环境下用户的动态加入与离开，通过广播加密的方式使域用户获得更新后的域密钥，避免了复杂的密钥更新协商协议。另外，提出基于共享域的电子文档管理协议，实现域内用户共享，不同域之间安全分发电子文档。在该协议工作下，共享域内每个用户合法获得的电子文档可以在域中各设备间无缝地流动，实现资源共享。不同的域之间电子文档的传输有严格的限制，需要经服务器认证，确保电子文档的安全管理与防泄密。

关键词：域；域密钥分发；广播加密；电子文档安全管理
中图分类号：TP309 **文献标识码：**A **文章编号：**1000-436X(2012)05-0012-09

Identity-based domain key distribution protocol in the E-document security management

YAN Xi-xi[1,2], MA Zhao-feng[1,2], YANG Yi-xian[1,2], NIU Xin-xin[1,2]
(1. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. Beijing National Security Science and Technology Co. Ltd, Beijing 100086, China)

Abstract: In order to create a security domain environment in th E-document management, an identity domain key distribution scheme using bilinear pairings for large and dynamic domain was proposed. The scheme could handle the joining and leaving of domain members efficiently, and updateed the domain key in the manner of broadcast, which avoided the complex protocols of key agreement. In addition, the distribution protocol based sharing-domain for E-document was also given, which aimed to realize the function of sharing the documents in a domain and distributing the documents between different domains securely. With the protocol, the E-documents obtained by a domain member could be transmitted to other domain members seamlessly. On the opposite, the E-document which was distributed to another domain need be upload to the server, which would verify the identi in member and encrypt the documents with the specified domain key.

Key words: domain; domain key distribution; broadcast and encrypt; E-document security management

1 引言

目前，办公网络化、自动化、电子化及信息资源共享已经成为社会发展的必然趋势。无纸化办公成为政府机构、学校和企事业单位信息化建设的重点，电子文档的使用越来越普及。然而，由于电子

收稿日期：2011-07-11；**修回日期：**2012-02-10
基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目（2007CB311203）；国家自然科学基金资助项目（60803157, 90812001）
Foundation Items: The National Basic Research Program of China (973 Program) (2007CB311203); The National Natural Science Foundation of China (60803157, 90812001)

文档的易复制、易分发、易扩散等特点决定了其不安全性，因此，电子文档安全管理与防泄密问题成为许多学者研究的热点之一。

快速发展的 Internet 技术使得电子文档需要在不同的用户之间流转，为了提高办公效率，用户往往会有一些特殊的需求：①许多相关用户作为一个用户组共享一些电子文档，允许用户设备的频繁加入/离开家庭网络；②用户拥有多台设备，想要使用其中任何一台设备访问电子文档，并且允许设备的离线使用。为了满足上述的要求，在电子文档管理中引入共享域概念。共享域内每个用户合法获得的电子文档可以在域中各设备间无缝地流动，实现资源共享。但是，不同的域之间电子文档的传输需要经服务器认证。

为了实现域间用户的通信安全，域成员之间需要建立一个共享的域密钥来加密域共享电子文档，因此，本文采用双线性对构造了一个新的基于身份的域密钥分发算法，该算法实现了域环境下用户的动态加入与离开，通过广播加密的方式使域用户获得更新后的域密钥，避免了复杂的密钥更新协商协议。另外，提出基于共享域的电子文档许可分发协议，实现域内用户共享，不同域之间安全分发电子文档。在该协议工作下，共享域内每个用户合法获得的电子文档可以在域中各设备间无缝地流动，实现资源共享；不同的域之间电子文档的传输有严格的限制，需要经服务器认证，确保电子文档的安全管理与防泄密。

2　相关工作

群通信系统中群密钥的管理主要分为 2 种分发机制：一种是群密钥分发机制，在这种方案中，群密钥是由一个主体(密钥分发中心)产生，并分发给每一个群成员；另一种是群密钥协商机制，每个用户负责生成一个秘密信息，然后利用各个用户所生成的秘密信息共同构造出共享的群会话密钥。

群密钥协商机制与群密钥分发机制相比，前者群密钥仅被群中的合法成员获得，具有更高的安全性和可靠性，同时无需可信赖机构，避免了分发机制中单一失效问题，适应于分布式网络环境。但是电子文档安全管理中，共享域可能存在大量的域共享用户，需要动态确定相应的密钥用户集合，保证域内授权的合法用户获得域密钥。密钥协商机制由于需要域内各个成员共同参与，计算量大，且交互信息多，增加了用户的负担。另外，域密钥仅被合法用户知道，服务端无法获取域密钥，不适应于电子文档安全管理中不同域之间文档的流转与分发。因此，本文主要采用群密钥分发机制实现电子文档的安全管理，该方案由密钥管理中心生成域密钥，并通过基于身份的域密钥分发机制将域密钥分发给域用户，允许任何用户任意时间的加入/撤离，应用灵活，算法简单，并减轻了用户的计算量。

目前已有的群密钥分发方案多是基于 Wong[1] 提出的逻辑树结构[2~4]，该方案应用于用户域变化不太大的情况下，可以达到很好的性能。文献[5]提出了单向函数树（OFT，one-way function trees）的群密钥管理方案，该方案基于单向函数构造密钥分发方案，树的每个叶节点代表一个群成员，根节点代表着群密钥，可以很好地适用于用户动态变化的共享域，降低了通信复杂度，但代价是存储复杂度的增大以及通信时延问题。Chou 和 Chen[6]提出基于中国剩余定理的“安全锁”方式将群密钥安全广播到每个群成员，然而局限于其高通信复杂性和计算复杂性，方案只能应用于小规模群组通信。文献[7~10]提出了一些基于身份的群密钥分发体制，Yang 等人在文献[9]中提出了一种基于身份的容错群密钥分发方案(IFCKDS)，服务端根据 n 个用户的签名采用秘密共享技术生成群密钥。文献[10]对 Yang 等人的方案进行改进，使其可以抵抗被动攻击，并具有前向安全性。

本文采用双线性对构造了一个新的基于身份的域密钥分发算法，该算法可高效地处理电子文档共享域中域成员加入，通过广播加密的方式使域用户获得更新后的域密钥，避免了复杂的密钥更新协商协议，适用于大规模、动态共享域环境下。

3　基本思想

电子文档共享域是拥有共同域密钥的所有设备，用于实现：将多个设备加入同一个域，统一管理设备及域的资源，通过域的机制实现资源共享，实现对域的管理，对域内设备的管理，同时保证域共享资源的安全。

同一部门中拥有的设备组成共享域，每个用户合法获得的电子文档可以在域中各设备间无缝地流动，实现资源共享。但是，不同的域之间电子文档的传输有严格的限制，需要经服务器认证。本文

提出一种基于身份的电子文档域密钥分发算法及协议，其特点如下。

1) 一旦共享域形成且用户终端加入共享域，该共享域中任何用户终端合法获得的电子文档和权限都可以与共享域中所有的用户终端共享，属于某个共享域的所有用户可以离线共享绑定到该域的版权，而不必重新向服务端申请。

2) 同一域内，采用用户标识和设备标识相结合的方式进行身份识别，实现权限控制。不同的用户角色拥有不同的权限，如域内普通用户只拥有阅读权限，域内管理员拥有阅读、打印、修改等权限，该方案有效地避免共享域中电子文档权限滥用，实现细粒度的访问控制。

3) 引入域证书，由服务端向用户发放域证书，用来控制共享域中用户对共享电子文档的使用。域证书包括域标识、管理者标识、管理者签名参数、域类型、发布时间以及管理者的签名。

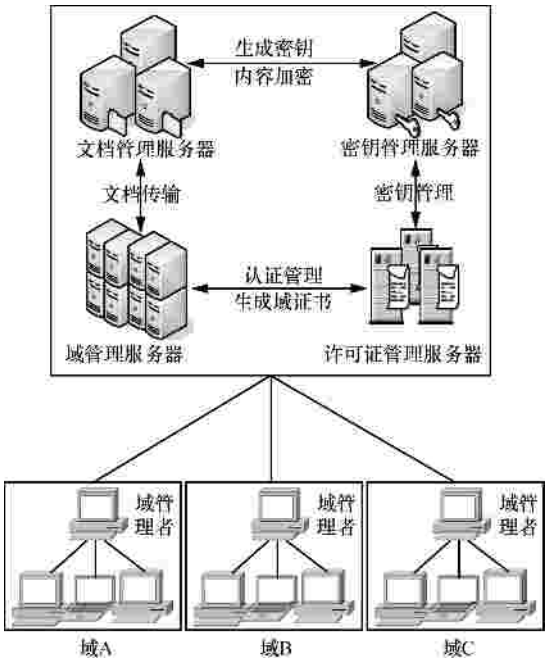

图1 电子文档域管理架构

4 域密钥分发算法

4.1 系统初始化

1) 系统参数生成

Step1 选择阶为素数q的循环加法群G_1，阶为素数q的循环乘法群G_2。$P \in G_1$是G_1的一个生成元。

Step2 选取一个双线性映射$e: G_1 * G_1 ? G_2$，对任意$P, Q, X \in G_1$，$a, b \in Z_q$满足：

$$e(aP, bQ) = e(P, Q)^{ab}$$

$$e(P+Q, X) = e(P, X)e(Q, X)$$

Step3 选择2个抗碰撞的杂凑函数H_1，H_2：$H_1 : \{0,1\}^* \to G_1$，$H_2 : G_2 \to \{0,1\}^l$，l为密钥的长度。

Step4 随机选择$s_1, s_2 \in Z_q^*$作为系统的主密钥。

2) 用户

Step1 用户$U_i, i = 1, 2, \text{L}, q$计算自己的身份信息$H_1(ID_i) \in G_1$，其中，$ID_i$为用户$U_i$的个人相关信息。

Step2 随机选取$x_i \in Z_q^*$，计算$Q_{ID_i} = x_i H_1(ID_i)$。

Step3 提交个人身份信息$ID_i \in \{0,1\}^*$和Q_{ID_i}给密钥生成中心(KGC, key generation center)。

Step4 用户可以向KGC证明其知道x_i，但不透露x_i的信息。

3) 密钥生成中心

Step1 随机选择$r \in Z_q^*$，计算$R = rP$，$R \in G_1$。

Step2 计算

$$U = R + \sum_{i=1}^{q} Q_{ID_i}$$

$$Z_i = s_1 H_1(ID_i) \in G_1$$

$$U_i = s_2\left(R + \sum_{j=1, j\neq i}^{q} Q_{ID_j}\right) \in G_1$$

Step3 KGC发送(U_i, Z_i)给用户U_i。

系统公开参数为$\{G_1, G_2, q, e, P, H_1, H_2\}$，系统秘密参数为$\{s_1, s_2, U\}$，由KGC秘密保管，用户$U_i$的解密密钥为$(U_i, Z_i, x_i)$。

4.2 域密钥分发

假定群密钥为s，KGC想把群密钥分发给每个域用户，进行如下操作。

Step1 KGC随机选择$t \in Z_q^*$。

Step2 计算$C_1 = s_2^{-1} tP \in G_1$，$C_2 = s_1^{-1} tP \in G_1$。

Step3 计算$g^t = e(U, P)^t \in G_2$，并计算$H_2(g^t) \in \{0,1\}^l$。

Step4 计算$C_3 = s \oplus H_2(g^t)$。

Step5 广播控制报头信息$H: (C_1, C_2, C_3)$。

4.3 域密钥恢复

Step1 用户收到广播信息H后，用户U_i应用其

个人解密密钥(U_i, Z_i, x_i)，计算

$W_1 = e(U_i, C_1)e(x_i Z_i, C_2)$。

Step2　计算$s = C_3 \oplus H_2(W_1)$，得到域密钥s。

4.4　新用户加入：域密钥更新

假定域D已经包含q个用户，申请加入的用户为U_{q+1}，其身份信息为ID_{q+1}。

1) 用户U_{q+1}

Step1　用户U_{q+1}计算自己的身份信息$H_1(ID_{q+1}) \in G_1$。

Step2　随机选取$x_{q+1} \in Z_q^*$，计算$Q_{ID_{q+1}} = x_{q+1}H_1(ID_{q+1})$。

Step3　提交个人身份信息$ID_{q+1} \in \{0,1\}^*$和$Q_{ID_{q+1}}$给KGC。

Step4　用户可以向 KGC 证明其知道x_{q+1}，但不透露x_{q+1}的信息。

2) KGC

Step1　随机选择$r' \in Z_q^*$，计算$R' = r'P \in G_1$。

Step2　计算$U = R' + \sum_{i=1}^{q+1} Q_{ID_i}$，$Z_{q+1} = s_1 H_1(ID_{q+1}) \in G_1$，$U_{q+1} = s_2\left(R' + \sum_{j=1}^{q} Q_{ID_j}\right) \in G_1$，$U_{\text{update}} = s_2(R' - R + Q_{ID_{q+1}})$。

Step3　发送(U_{q+1}, Z_{q+1})给用户U_{q+1}，并广播密钥更新算子U_{update}。

Step4　用户U_{q+1}的解密密钥为$(U_{q+1}, Z_{q+1}, x_{q+1})$。

Step5　系统的加密密钥为$\{s_1, s_2, U'\}$。

3) 其余q个用户

用户$U_i, i = 1, 2, \ldots, q$　计算$U_i' = U_i + U_{\text{update}}$。

用户$U_i, i = 1, 2, \ldots, q$的解密密钥为(U_i', Z_i, x_i)。

4.5　域密钥更新

Step1　用户U_i应用其个人解密密钥(U_i', Z_i, x_i)，计算$W_2 = e(U_i', C_1)e(x_i Z_i, C_2)$。

Step2　计算$s = C_3 \oplus H_2(W_1) \oplus H_2(W_2)$，得到域密钥$s$。

5　电子文档域管理协议

5.1　系统参数定义

系统参数定义如表 1 所示。

表 1　系统参数定义

参数名称	参数定义
DS	域服务器
CS	许可证服务器
KS	密钥服务器
Database_S	数据库服务器
pk_s	服务端公钥
sk_s	服务端私钥
pk_u	用户公钥
sk_u	用户私钥
dk_U	用户解密域密钥的密钥

5.2　域创建及注册协议

Step1　域创建者A向域管理服务器提交建立一个新域的申请，发送用户名AID及设备硬件信息CID。

A->DS: E_{pk_S} (*AID* || *CID* || *Request_CreatDomain*)

Step2　服务端域管理服务器收到申请后，解密获得用户A的用户名AID及设备信息CID，查询该终端是否归属于某个域，如未有归属的域，则同意用户A的申请；否则拒绝申请。

DS：$D_{\text{sk\_S}}$ (AID || CID || CreateDomain Request)

If ($AID \notin DID$)　Agree the request

Else　refuse the request

Step3　域创建者收到服务端的响应后，发送域标识符(DID)，域用户列表Potential_user list等参数给服务端。

A->DS：$E_{\text{pk\_S}}$ (DID || Potential_user list)

Step4　服务端收到用户列表后，对域DID进行域的参数设置，并创建设备域DID的列表：设备申请调入域列表、潜在设备入域列表以及用户设备列表，域DID创建完成。

DS: creat (Applying_user list || Potential_user list|| Domain_user list)

Step5　DS发送域创建成功响应级用户A。

DS-> A: Success_response

5.3　用户入域协议

用户申请入域协议主要用于用户设备加入共享域，新的用户设备加入域后，密钥管理器需要进行域密钥更新，域管理器需要生成新的域证书分发给域内所有用户，并提交更新的信息给数据库服务器。

用户设备申请入域有2种方式：①用户向服务端申请入域时，已经是潜在用户设备列表中的用户，则不需要域管理者进行在线审核，直接入域，服务端将用户设备信息添加到域用户设备列表；②用户设备不是潜在用户设备列表中的用户，向服务端发出申请入域请求，用户设备信息将被添加到设备申请入域列表，由域管理者对其设备信息进行在线审核，审核通过后，服务端将用户设备加入到域用户设备标识列表中。

Applying_user list：设备申请入域列表。当设备申请入域时，服务端将设备信息记录到设备申请入域列表，由域管理者进行在线审核设备是否有资格加入域。

Potential_user list：潜在设备入域列表。由域管理者创建，当用户申请入域时，DS将检索潜在设备入域列表，如果存在，则直接接受用户入域请求，而无需返回给域管理者审核；如果不在，则将用户信息记录到设备申请入域列表。

Domain_user list：域用户设备列表。记录域中所有的用户，当用户设备成功入域后，用户设备将被添加到用户设备列表，用于生成域证书。

Step1 用户U向服务端发送入域申请，提交用户标识（UID）（包含个人身份信息 $ID_i \in \{0,1\}^*$ 和 Q_{ID_i}）、设备信息（CID）、以及申请加入的域标识DID。

U->DS: E_{pk_S}(Request_JoinDomain || UID || CID || DID)

Step2 DS解密获得用户信息，验证用户提交的信息，检索用户是否存在于Potential_user list。

1) 如果不存在，则：

① DS：将用户设备信息添加到设备申请入域列表，等待域管理者在线审核，返回等待信号给用户U。

DS->A：Update Applyinguser_list

DS->A：Wait response

② A：解密获得用户信息，审核用户U的信息，通过用户UID及CID判断用户是否有资格加入域DID，将审核结果返回给DS。

③ DS：如果审核通过，则更新*Domain_user list*；否则，将拒绝用户U的申请。

DS：Update Domain_user list

2) 如果存在于用户列表，则进行Step 3。

Step3 域证书分发阶段。

1) DS：将用户U的UID和CID提交给KS，调用域密钥分发算法，生成用户U的个人解密密钥dk_U，上传给CS。

2) CS：由CS为域DID生成域证书D_License。

D_License={DID‖SID‖AID‖User_list‖Pub_time‖dk_U}。

3) DS：DS对域证书进行签名，并以用户U的公钥进行加密，传输给U。

DS -> U: E_{pk_A} (Sig_{DS}(D_License))

4) Database_S：将域ID、域证书发放时间、域用户列表及相关参数、域版本号写入数据库。

5) DS：广播密钥更新算子 U_{update}。

Step4 域密钥恢复阶段。

1) 用户U使用自己的私钥解密获得域证书，并通过DS的公钥验证证书的签名，若验证通过，则接受证书，否则拒绝接受。

U: D_{sk_A} (Sig_{DS}(D_License))

2) 用户通过个人解密密钥dk_U，获得域密钥。

3) 域内其他用户设备在下次上线时，将通过域密钥更新算子 U_{update}，更新自己的解密密钥。

4) 通过域密钥更新算法 $s = C_3 \oplus H_2(W_1) \oplus H_2(W_2)$，获得域密钥。

5.4 用户撤域协议

用户撤域主要存在2种情况：①用户主动申请撤域；②用户被动撤域，服务端强制性要求用户退出域。用户撤域后，密钥管理器需要进行域密钥更新，域管理器需要生成新的域证书分发给域内所有用户，并提交更新的信息给数据库服务器。

Step1 申请阶段。

1) 用户主动申请撤域

① 用户U向服务端发送撤域申请，提交UID、CID以及申请退出的DID。

U->DS: E_{pk_S}(Request_ExitDomain || UID || CID || DID)

② DS解密获得用户信息，验证用户提交的信息，检索用户信息是否存在于域DID用户列表内。如果未存在，则返回错误信息给用户，终止该协议；否则，执行域证书更新阶段。

2) 用户被动撤域

DS向用户U发出离域通知，并从域用户列表中删除其设备信息。

Step2 域证书更新阶段。

1) DS：将更新后的域用户设备信息，提交由KS更新域密钥key_Domain，上传给CS。

2) CS：由CS为域DID生成域证书D_License。

D_License={*DID*||*SID*||*AID*||*User_list*||*Pub_time*||*key_Domain* }

3) DS：DS对域证书进行签名。*DS: Sig*$_{DS}$(*D_License*)。

4) Database_S：将域ID、域证书发放时间、域用户列表及相关参数、域版本号写入数据库。

Step3　证书发放阶段。

域内其他用户设备在下次上线时，DS将发送新的域证书给用户。

DS -> U_1, U_2, U_3,…, U_n: *D_License*= {DID||SID||AID||User_list||Pub_time||key_Domain }

6　协议安全性分析

6.1　正确性

1) 用户域密钥恢复正确性分析

本方案中用户收到广播信息后，需要利用自己的解密密钥，通过计算 $W_1 = e(U_i, C_1)e\left(x_i Z_i, C_2\right)$，恢复出域密钥。

$$
\begin{aligned}
&e(U_i, C_1)e\left(x_i Z_i, C_2\right)\\
&= e\left(s_2\left(U - Q_{ID_i}\right)s_2^{-1}tP\right)e\left(x_i s_1 H_1\left(ID_i\right), s_1^{-1}tP\right)\\
&= e\left(\left(U - Q_{ID_i}\right), tP\right)e\left(Q_{ID_i}, tP\right)\\
&= e\left(U, tP\right)e\left(-Q_{ID_i}, tP\right)e\left(Q_{ID_i}, tP\right)\\
&= e\left(U, tP\right)\\
&= e\left(U, P\right)^t\\
&= g^t
\end{aligned}
$$

由 $s = C_3 \oplus H_2\left(g^t\right)$ 正确计算出域密钥 s。

2) 用户 $U_i, i = 1, 2, \text{L}, n$ 的解密密钥更新正确性分析

当新的用户加入域时，密钥服务器为新用户生成个人的解密密钥，同时发布密钥更新算子，其余用户根据密钥更新算子，计算出自己新的解密密钥。

$$
\begin{aligned}
&U_i'\\
&= U_i + U_{\text{update}}\\
&= s_2\left(R + \sum_{j=1, j\neq i}^{q} Q_{ID_j}\right) + s_2\left(R' - R + Q_{ID_{n+1}}\right)\\
&= s_2\left(R' + \sum_{j=1, j\neq i}^{q} Q_{ID_j} + Q_{ID_{q+1}}\right)\\
&= s_2\left(R' + \sum_{j=1, j\neq i}^{q+1} Q_{ID_j}\right)
\end{aligned}
$$

$$
\begin{aligned}
&U_i'\\
&= s_2\left(U - Q_{ID_i}\right)\\
&= s_2\left(R' + \sum_{i=1}^{q+1} Q_{ID_i} - Q_{ID_i}\right)\\
&= s_2\left(R' + \sum_{j=1, j\neq i}^{q+1} Q_{ID_j}\right)
\end{aligned}
$$

由 $U_i' = s_2(U - Q_{ID_i}) = U_i + U_{\text{update}}$ 推出用户 $U_i, i = 1, 2, \text{L}, q$ 解密密钥更新正确。因此，基于身份的域密钥分发算法是正确的。

6.2　安全性分析

1) 在 BDH（双线性 Diffie-Hellman 问题）和 ECDLP（椭圆曲线离散对数问题）等计算困难性假设下，基于身份的域密钥分发算法和协议是安全的。

证明　假设协议参与方为密钥生成中心 KGC、用户集 $\{U_1, U_2, \text{L}, U_q\}$、敌手 E。

① 假设敌手 E 为非域中成员，采取主动攻击方式向 KGC 发送申请域密钥请求，并提交个人 UID。KGC 收到敌手的申请请求后，解密获得用户信息，验证用户提交的信息，检索用户是存在于潜在设备入域列表 Potential_user list。必然，敌手 E 并不存在于潜在设备入域列表。因此，攻击者将无法通过 KGC 服务器的验证，无法获得域密钥。

② 假设敌手 E 为非域中成员，获得广播信息 (C_1, C_2, C_3) 和系统公开参数 $\{G_1, G_2, q, e, P, H_1, H_2\}$，要想获得域密钥 s，由上述算法中 $s = C_3 \oplus H_2\left(g^t\right)$ 可知，域密钥 s 与 $g^t = e(U_i, C_1)e\left(x_i Z_i, C_2\right) = e\left(U, P\right)^t$ 有关。

在 ECDLP 问题计算困难性假设下，敌手 E 无法从 $C_1 = s_2^{-1}tP \in G_1$，$C_2 = s_1^{-1}tP \in G_1$ 中计算出 $s_2^{-1}t$ 和 $s_1^{-1}t$，更无法计算出 t。因此，无法计算出 g^t，相当于无法获得域密钥 s。

敌手 E 在没有 KGC 分发的用户解密密钥 (U_i, Z_i, x_i) 或者系统秘密参数 U 的情况下，仅仅从广播信息 (C_1, C_2, C_3) 和系统公开参数 $\{G_1, G_2, q, e, P, H_1, H_2\}$ 计算出 g^t 是不可行的。

③ 假设敌手 E 为域中成员，即敌手 E 拥有解密密钥 (U_i, Z_i, x_i) 和广播信息 (C_1, C_2, C_3)，根据椭圆曲线离散对数问题（ECDLP）的难解性，对给定的 $Q = xP \in G$，计算 $x \in Z_q^*$ 是困难的。敌手 E 从 $U_i = s_2\left(R + \sum_{j=1, j\neq i}^{q} Q_{ID_j}\right) \in G_1$，$Z_i = s_1 H_1\left(ID_i\right) \in G_1$ 计算

得出 $s_1, s_2 \in Z_q^*$ 是困难的。因此，敌手 E 无法根据解密密钥 (U_i, Z_i, x_i) 和广播信息 (C_1, C_2, C_3) 获得 KGC 的任何信息。

综上所述，在 BDH 和 ECDLP 等计算困难性假设下，基于身份的域密钥分发算法和协议是安全的。

2) 抗合谋攻击：系统中共享域用户的合谋不能产生一个有效的解密密钥，即该方案可以有效抵御域用户合谋攻击。

假设有 m 个域用户合谋，即假定 m 个域用户成员利用各自的解密密钥 (U_i, Z_i, x_i) 对系统进行合谋攻击。

①根据椭圆曲线离散对数问题由用户解密密钥 (U_i, Z_i, x_i) 从 $U_i = s_2\left(R + \sum_{j=1, j\neq i}^{q} Q_{ID_j}\right) \in G_1$，$Z_i = s_1 H_1(ID_i) \in G_1$ 计算得出 $s_1, s_2 \in Z_q^*$ 是困难的。

②m 个合谋用户利用各自的 Q_{ID_i} 相加，由于随机数 $r \in Z_q^*$ 的存在，无法计算出 $R = rP$，增加了用户计算 U 的难度。

③根据基于双线性对的计算困难性问题，合谋用户从 $e(U, P)^s$ 也不能计算出 U。

因此，合谋用户无法获得系统主密钥 $s_1, s_2 \in Z_q^*$ 或系统秘密参数 U，即不能产生新的有效用户解密密钥。

7 应用场景

7.1 域内用户共享电子文档

电子文档经常需要在同一部门内流通，通过共享域来实现域内用户共享电子文档，一旦共享域形成且用户终端加入共享域，该共享域中任何用户终端合法获得的电子文档和权限都可以与共享域中所有的用户终端共享，属于某个共享域的所有用户可以离线共享绑定到该域的版权，而无需每次都向服务端申请解密，减轻了网络的负担，避免服务端负荷过载；同时，解决了移动设备离线使用电子文档的问题，实现同一用户在多个设备上使用电子文档。

假定用户A与用户B为同一共享域内用户，电子文档共享流程如图2所示。

1) 用户A合法获得电子文档D，本地客户端透明加密存储。

2) 客户端通过内容密钥解密电子文档。

3) 用户A采用域密钥加密电子文档，转发给用户B。

4) 用户B客户端通过域密钥解密获得电子文档，并采用本地内容密钥加密文档。

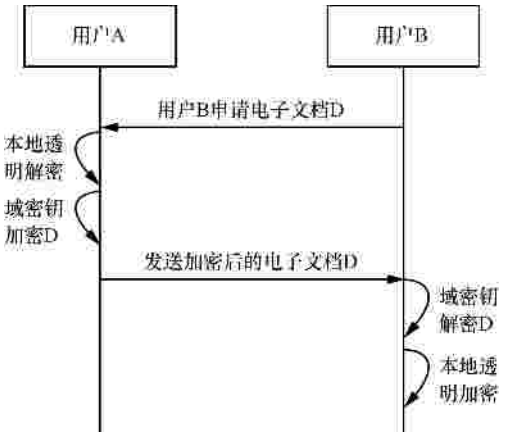

图2 域内用户共享电子文档流程

7.2 跨域用户之间分发电子文档

假定用户A与用户B为不同的域用户，电子文档转发流程如图3所示。

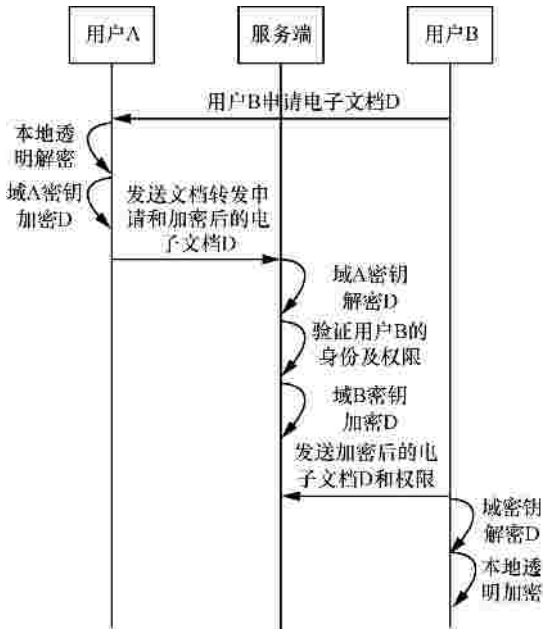

图3 跨域用户电子文档分发流程

1) 用户A合法获得电子文档D，本地客户端透明加密存储。

2) 用户B向用户A申请电子文档。

3) 用户A客户端通过内容密钥解密电子文档，采用域密钥加密电子文档。

4) 用户A向服务端发出转发电子文档申请，并设置用户B的文档权限，上传电子文档与权限给服

务端。

5) 服务端解密获得电子文档明文与权限，并从数据库服务端获得用户B的角色，判断用户A为用户B设置的文档权限是否符合用户B的角色($rights \in B\_role$)，如果符合，则确定用户B对电子文档的权限；否则，重新设置用户B对电子文档的权限。

6) 服务端从密钥数据库中提取用户B所在域的域密钥，由内容打包服务器加密打包电子文档与权限，发送给用户B。

7) 用户B解密获得电子文档，并根据权限控制使用电子文档。

8 与其他方案比较

该算法中，假定有 n 个用户，基于身份的电子文档域密钥分发方案的通信复杂度为 $O(1)$，KGC 的密钥复杂度为 $O(n)$，用户的存储复杂度为 $O(1)$，计算复杂度为 $2T_{\mathrm{M}}+3T_{\mathrm{DM}}+2T_{\mathrm{e}}$。

假定 T_{e} 表示一次双线性映射运算所需的时间；T_{DM} 表示椭圆曲线中一次点乘运算所需的时间；T_{M} 表示 Z_q^* 中一次模乘运算所需的时间；忽略运算量较小的运算和异或操作所需的时间开销散列，基于身份的域密钥分发算法计算代价如表2所示。

表 2　基于身份的域密钥分发算法计算代价

算法过程	计算代价
域密钥分发过程	$2T_{\mathrm{M}}+2T_{\mathrm{DM}}+T_{\mathrm{e}}$
域密钥恢复过程	$T_{\mathrm{DM}}+2T_{\mathrm{e}}$
总计	$2T_{\mathrm{M}}+3T_{\mathrm{DM}}+3T_{\mathrm{e}}$

如果广播中心选择相同的生成元 P，预先计算 $e(U, P)$，则可在以后的域密钥加密过程中不再进行双线性映射运算，则计算代价可以降低到 $2T_{\mathrm{M}}+3T_{\mathrm{DM}}+2T_{\mathrm{e}}$。

当用户离开或加入时，KGC 只需要广播一组广播分组，域用户只需要做一次点加操作，减少了密钥更新量和分发的复杂性。

与单向函数树的群密钥管理方案、文献[10]的基于身份的群密钥分发机制、群密钥协商机制比较，该方案在存储复杂度、通信复杂度、计算复杂度、适用环境比较结果如表 3 所示。

表 3　与其他域密钥管理方案比较

比较类别	本文方案	OFT 方案[5]	IFCKDS 方案[10]	群密钥协商方案
采用的密码算法	双线性对	单向函数	双线性对	公钥密码
存储复杂度（KGC）	$O(n)$	$O(n)$	$O(n)$	$O(n)$
存储复杂度(域成员)	$O(1)$	$O(\log n)$	$O(n)$	$O(1)$
成员加入广播消息长度	$O(n)$	$O(\log n)$	$O(nk)$	$O(n^2)$
需要密钥管理中心	Y	Y	Y	N
支持域组成员的数量	任意大小	任意大小	任意大小	小
适用环境	高度集中，也适用于分布式	高度集中	分布式	高度集中，也适用于分布式

9 结束语

针对共享域环境下电子文档安全管理系统中用户的通信安全，本文采用双线性对构造了一个基于身份的域密钥分发算法及协议，具备以下4个优点：①共享域内每个用户合法获得的电子文档可以在域中各设备间无缝地流动，实现资源共享；②不同的域之间电子文档的传输有严格的限制，需要经服务器认证，确保电子文档的安全管理与防泄密；③共享域中的用户可以离线使用电子文档；④采用用户标识和设备标识相结合的方式进行身份识别，实现对电子文档的细粒度使用控制。域密钥管理研究仍存在很多值得深入研究的问题，在后续的工作中将对该方法进行改进，以支持更为高效的域密钥管理机制。

参考文献：

[1] WONG C K, GOUDA M, LAM S S. Secure group communications using key graphs[J]. IEEE Tran Networks, 2000, 8(8): 16-30.

[2] WALLNER D M, HARDER E J, AGEE R C. Key management for multicast: issues and architectures[J]. Computer and Information Science, 1999, (7): 1-23.

[3] WALDVOGEL M, CARONNI G, SUM D, *et al*.The versa key framework: versatile group key management [J]. IEEE Jo nal on Selected Areas in Communications (Special Issue on Middleware), 1999, 17(9):1614-1631.

[4] SHEMAN A T, ACGREW D A. Key establishment in large dynamic groups using one-way function trees[J]. IEEE Transactions on Software Engineering, 2003, 29 (5): 444-458.

[5] DINSMORE P T, BALENSON D M, HEYMAN M, *et al*. Policy-based security management for large dynamic groups: an overview of the DCCM project[A]. Proc the DARPA Information Sur ivability Conference &Exposition[C]. SC, USA, 2000. 64-73.

[6] CHOU G H, CHEN W T. Secure broadcasting using the secure lock

[J]. IEEE Trans on Software Engineering, 1989, 15(8): 929-934.

[7] WANG T H, CHEN J L. Identity-based conference key broadcast systems[J]. IEEE Proc of Computers and Digital Techniques, 1994, 141(l): 57-60.

[8] CHIKAZAWA T, YAMAGISHI A. An improved identity-based one-way conference key sharing system[A]. Proc of ICCS/ISITA[C]. IEEE Computer Society Press, 1992. 270-273.

[9] YANG Z K, XIE H T, CHEN W Q, *et al*. An identity-based fault-tolerant conference key distribution scheme[A]. The 7t International and Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06)[C]. 2006. 389-392.

[10] CAI Y Q, LI X Y. An Improved identity-based fault-tolerant conference key distribution scheme[A]. Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing[C]. 2007.345-349.

[11] **蒙杨，刘克龙，卿斯汉**. **可扩展的多级会议密钥分发体制**[J]. **计算机学报**,2000,23(8):793-798.
MENG Y, LIU K L, QING S H. A scalable key distribution system for multilevel security conference[J]. Chinese Journal of Computers, 2000, 23(8):793-798.

[12] **李先贤，怀进鹏，刘旭东**. **群密钥分配的动态安全性及其方案**[J]. **计算机学报**,2002, 25(4):337-345.
LI X X, HUAI J P, LIU X D. Dynamic security of group key distribution and its solutions[J]. Chinese Journal of Computers, 2002, 25(4): 337-345.

[13] **孙海波，林东岱**. **基于零知识集的群组密钥分配方案**[J]. **电子学报**,2005, 33(2):345-349.
SUN H B, LIN D D. A new group key exchange protocol based on zero-knowledge set[J]. Chinese Journal of Electronics, 2005, 33(2): 345-349.

[14] **徐守志，杨宗凯**.**多服务安全组播组密钥管理技术研究**[D]. **武汉**: **华中科技大学，**2006.
XU S Z, Y Z K. Research on Group Key Management Technology of Multi-Service Secure Multicast[D]. Wuhan: Huazhong Unversity of Science and Technology, 2006.

[15] **汪小芬，肖国镇**. **认证密钥协商协议的研究**[D]. **西安**: **西安电子科技大学**,2009.
WANG X F, XIAO G Z. Study on Authenticated Key Agreeme t Protocols [D]. Xi'an: Xidian University, 2009.

[16] **张雅哲，徐海霞，李宝**. **可否认群密钥协商协议的一般化构造方式**[J]. **通信学报**, 2011, 32(3): 143-149.
ZHANG Y Z, XU H X, LI B. Generic construction of deniable group key establishment from group key establishment[J]. Journal on Communications, 2011, 32(3):143-149.

作者简介：

闫玺玺（1985-），女，河南灵宝人，北京邮电大学博士生，主要研究方向为数字版权管理、数字内容安全和计算机网络安全。

马兆丰（1974-），男，甘肃镇原人，博士，北京邮电大学副教授，主要研究方向为数字版权管理、数字内容安全和计算机网络安全。

杨义先（1961-），男，四川盐亭人，北京邮电大学教授、博士生导师，主要研究方向为密码学、计算机网络与信息安全。

钮心忻（1963-），女，浙江湖州人，北京邮电大学教授、博士生导师，主要研究方向为数字水印、信息隐藏和隐写分析。