ICS 35.040
L 80

中华人民共和国国家标准

GB/T 34953.2—2018/ISO/IEC 20009-2:2013

信息技术　安全技术　匿名实体鉴别
第 2 部分:基于群组公钥签名的机制

Information technology—Security techniques—Anonymous entity authentication—Part 2:Mechanisms based on signatures using a group public key

(ISO/IEC 20009-2:2013,IDT)

2018-09-17 发布　　2019-04-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　符号和缩略语 …… 3
5　模型和需求 …… 4
6　密钥产生过程 …… 4
7　无在线可信第三方参与的匿名鉴别机制 …… 5
7.1　概述 …… 5
7.2　单向匿名鉴别 …… 6
7.3　双向匿名鉴别 …… 7
7.4　单向匿名双向鉴别 …… 10
7.5　带有绑定特性的双向匿名鉴别 …… 12
7.6　带有绑定特性的单向匿名双向鉴别 …… 17
8　有在线可信第三方参与的匿名鉴别机制 …… 22
8.1　概述 …… 22
8.2　单向匿名鉴别 …… 22
8.3　双向匿名鉴别 …… 25
8.4　单向匿名双向鉴别 …… 28
9　群组成员打开过程 …… 35
9.1　总则 …… 35
9.2　证据评价过程 …… 36
10　群组签名连接过程 …… 36
10.1　总则 …… 36
10.2　与打开方的连接过程 …… 36
10.3　带有连接密钥的连接过程 …… 37
10.4　带有连接库的连接过程 …… 37
附录 A（规范性附录）　对象标识符 …… 38
附录 B（资料性附录）　具有绑定属性的机制的信息 …… 39
参考文献 …… 40

前　　言

GB/T 34953《信息技术　安全技术　匿名实体鉴别》已发布或计划发布以下部分：

——第 1 部分：总则；

——第 2 部分：基于群组公钥签名的机制；

——第 3 部分：基于盲签名的机制；

——第 4 部分：基于弱秘密的机制。

本部分为 GB/T 34953 的第 2 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分使用翻译法等同采用 ISO/IEC 20009-2:2013《信息技术　安全技术　匿名实体鉴别　第 2 部分：基于群组公钥签名的机制》。

与本部分中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 34953.1—2017　信息技术　安全技术　匿名实体鉴别　第 1 部分：总则(ISO/IEC 20009-1:2013,IDT)。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：西安西电捷通无线网络通信股份有限公司、无线网络安全技术国家工程实验室、WAPI 产业联盟(中关村无线网络安全产业联盟)、国家密码管理局商用密码检测中心、重庆邮电大学、国家无线电监测中心检测中心、中国电子技术标准化研究院、天津市无线电监测站、中国通用技术研究院、北京大学深圳研究生院、中国科学院软件研究所、国家计算机网络应急技术处理协调中心、中国网络空间研究院、国家信息技术安全研究中心、国家信息安全工程技术研究中心、中国人民解放军信息安全测评认证中心、公安部第三研究所、北京计算机技术及应用研究所、福建省无线电监测站、北京数字认证股份有限公司、中国电信股份有限公司上海研究院、工业和信息化部宽带无线 IP 标准工作组。

本部分主要起草人：杜志强、曹军、黄振海、李大为、宋起柱、李琴、龙昭华、冯登国、舒敏、陈晓桦、李京春、葛培勤、郭晓雷、高波、朱跃生、李广森、顾健、李楠、于光明、张璐璐、铁满霞、张变玲、许玉娜、胡亚楠、颜湘、张国强、童伟刚、李明、万洪涛、王月辉、郑骊、彭潇、朱正美、陈志宇、侯鹏亮、许福明。

引　言

GB/T 34593 的本部分定义了基于群组公钥签名的匿名实体鉴别机制，分为有在线可信第三方参与的鉴别机制和无在线可信第三方参与的鉴别机制两类。

本文件的发布机构提请注意，声明符合本文件时，可能涉及第 8 章与 ZL201010546339.3、ZL201010546320.9、CN201210063055.8、CN201210063632.3、CN201210063650.1、ZL200910024191.4、ZL200910023774.5、ZL200910023735.5 等相关的专利的使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构保证，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本文件发布机构备案。相关信息可通过以下联系方式获得：

专利持有人姓名：西安西电捷通无线网络通信股份有限公司

地址：西安市高新区科技二路 68 号西安软件园秦风阁 A201

联系人：冯玉晨

邮政编码：710075

电子邮件：ipri@iwncomm.com

电话：029-87607836

传真：029-87607829

网址：http://www.iwncomm.com

本文件的发布机构提请注意，本文件等同采用 ISO/IEC 20009-2:2013，因此，除上述声明外，韩国电子通信研究院、英特尔公司针对 ISO/IEC 20009-2:2013 所作出的“专利持有人愿意基于无歧视、合理条件和条款与其他方协商许可”的声明适用于本文件。相关信息可通过以下联系方式获得：

专利持有人姓名：Electronics and Telecommunications Research Institute

地址：161，Gajeong-dong，Yuseong-gu，Daejeon，305-700，KOREA

联系人：Hanchul Shin

电子邮件：vip123@etri.ke.kr

电话：+82-042-860-5797

传真：+82-042-860-3831

网址：http://www.etri.re.kr

专利持有人姓名：Intel Corporation

地址：Intel Legal and Corporation Affairs 2200 Mission College Blvd.，RNB-150，Santa Clara，CA 95054

联系人：James Kovacs

电子邮件：Standards.Licensing@intel.com

电话：408-765-1170

传真：408-613-7292

网址：http://www.intel.com/standards/licensing.html

请注意除上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

信息技术　安全技术 匿名实体鉴别 第2部分:基于群组公钥签名的机制

1　范围

GB/T 34953的本部分定义了基于群组公钥签名的匿名实体鉴别机制,验证方基于群组签名机制验证对端身份的合法性且不需要获得对端的身份信息。

本部分规定了:

——基于群组公钥签名的匿名实体鉴别机制的通用描述;

——多种匿名鉴别机制。

本部分描述了:

——群组成员发布过程;

——无在线可信第三方参与的匿名实体鉴别机制;

——有在线可信第三方参与的匿名实体鉴别机制。

另外,本部分还规定了:

——群组成员身份打开的过程(可选);

——群组成员签名连接的过程(可选)。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

ISO/IEC 20008-1 信息技术　安全技术　匿名签名服务　第1部分:总则(Information technology—Security techniques—Anonymous digital signatures—Part 1:General)

ISO/IEC 20008-2 信息技术　安全技术　匿名签名服务　第2部分:采用群组公钥的机制(Information technology—Security techniques—Anonymous digital signatures—Part 2:Mechanisms using a group public key)

ISO/IEC 20009-1 信息技术　安全技术　匿名实体鉴别　第1部分:总则(Information technology—Security techniques—Anonymous entity authentication—Part 1: General)

3　术语和定义

ISO/IEC 20008-1、ISO/IEC 20009-1 界定的以及下列术语和定义适用于本文件。

3.1

绑定属性　binding-property

在通信实体的消息间提供绑定保证的属性。

3.2

认证机构　certification authority

受信任的创建和颁发公钥证书的实体。

[ISO/IEC 11770-1:2010,定义2.3]

3.3

临时密钥对　ephemeral key pair

由一个临时公钥和一个临时私钥构成的一个非对称密钥对，该临时公钥和临时私钥对一个加密方案的每次执行过程均是惟一的。

3.4

群组公钥证书　group public key certificate

由证书认证机构签发的群组的公钥信息。

3.5

群组公钥认证机构　group public key certification authority

被信任用于创建和分配群组公钥证书的实体。

3.6

群组公钥信息　group public key information

该信息至少包含群组可区分标识符和群组公钥，而且也能包含关于群组公钥认证机构、群组、密钥使用限制、有效期以及相关算法等其他静态信息。

3.7

密钥导出函数　key derivation function

以共享秘密和其他互相都知道的参数作为输入，输出用做密钥的一个或多个共享秘密的函数。

[ISO/IEC 11770-3:2015，定义 3.22]

3.8

本地连接能力　local linking capability

具备如下特征的连接能力，来源于相同匿名用户的两个或多个签名仅被特定的群组签名连接器通过一个连接密钥连接，而其他实体则不能连接上述签名。

3.9

消息鉴别码　message authentication code；MAC

消息鉴别码算法输出的比特串。

[ISO/IEC 9797-1:2011，定义 3.9]

3.10

消息鉴别码(MAC)算法　message authentication code (MAC)algorithm

一种算法，用于计算将比特串和秘密密钥映射为定长比特串的函数，并满足以下两种性质：

——对任意密钥和任意输入串，该函数能被有效计算；

——对任一固定的密钥，该密钥在未知情况下，即便已知输入串和对应函数值的集合(其中第 i 个输入串的值可以在观察前 $i-1$ 个函数值的值之后被选定)，计算任何新输入串的函数值在计算上也是不可行的。

[ISO/IEC 9797-1:2011，定义 3.10]

3.11

公钥证书　public key certificate

由证书认证机构签发的实体的公钥信息。

[ISO/IEC 11770-1:2010，定义 2.37]

3.12

公钥信息　public key information

该信息至少包含实体可区分标识符和公钥，而且也能包含关于认证管理机构、实体、密钥使用限制、有效期以及相关算法等其他静态信息。

[ISO/IEC 11770-1:2010，定义 2.38]

4 符号和缩略语

下列符号和缩略语适用于本文件。

A	实体 A 的可区分标识符
B	实体 B 的可区分标识符
$Cert_A$	实体 A 的公钥证书
$Cert_B$	实体 B 的公钥证书
$Cert_G$	群组 G 的群组公钥证书
G,G'	群组 G 或 G' 的可区分标识符
G	q 阶循环群，其中的判定性 Diffie-Hellman(DDH)问题是难解的
g	G 的生成元
$gsS_{XG}(m)$	实体 X 使用群组公钥生成的匿名签名，该签名是实体 X 应用了一种本部分规定的群组签名机制、使用群组成员签名密钥 S_{XG} 对待签名消息 m 的签名
I_G	群组 G 的身份，可以用 G 或 $Cert_G$ 表示
I_X	群组 X 的身份，可以用 X 或 $Cert_X$ 表示
kdf	密钥导出函数
MAC	消息鉴别码
m	待签名消息
$mac_K(M)$	使用密钥 K 和一个任意数据串 M 的 MAC 算法
N_X	由实体 X 颁发的序列号
P_A	实体 A 的公钥
P_B	实体 B 的公钥
P_G	群组 G 的群组公钥
q	素数
Res_A	验证实体 A 的公钥或公钥证书的结果
Res_B	验证实体 B 的公钥或公钥证书的结果
Res_G	验证群组 G 的群组公钥或群组公钥证书的结果
R_X	实体 X 产生的随机数
S_{XG}	与实体 X 关联的群组成员签名密钥，实体 X 是群组 G 的一个成员
$sS_X(m)$	实体 X 用其签名私钥对消息 m 生成的数字签名
TP	TTP 的可区分标识符
TTP	可信第三方
T_X	实体 X 颁发的时间戳
Z_q	$[0,q-1]$之间的整数集
$\|$	$Y \| Z$ 用于表示数据项 Y 和 Z 以指定的顺序串联的结果。当两个或多个数据项的串联结果作为一种本部分指定的机制的输入时，这个结果应能够被惟一的分解成其构成时的数据项的一个组合，这样才不会导致存在含糊不清的解释的可能。后面的这个属性根据具体的应用存在多种不同的实现方式。例如，它可以采用以下两种方式： a) 在整个机制的使用过程中固定每个数据项的长度； b) 使用能够确保解码惟一性的串联数据项的序列编码方法，如 ISO/IEC 8825-1 [1]中使用的区别性编码规则。

5 模型和需求

本章描述了匿名鉴别机制涉及的模型和需求。

一个基于群组公钥签名的实体鉴别机制通常包含一系列的群组成员。每个群组一定有一个群组成员发布方。如果有必要通过打开在鉴别协议中产生的一个群组签名来揭露它的声称方,一个群组应有一个群组的打开方。一个群组如果有必要连接同一声称方出于鉴别的目的产生的两个群组签名,也可能要有一个连接方。这个机制的匿名强度取决于这个群组的群组成员数量,一个匿名的实体鉴别机制被定义为如下规范流程:

——密钥的产生过程;

——匿名实体的鉴别过程;

——打开过程(如果机制支持打开);

——连接过程(如果机制支持连接)。

正如以下定义,本部分中使用到了各种各样的实体,有些实体在所有的机制中都会涉及,而其他一些实体只在部分机制中才涉及。在本部分中,如果一个机制支持打开或者连接,则其使用的相关操作过程所遵循的群组签名方案见 ISO/IEC 20008-2。

——声称方(Claimant):一个在被鉴别时其身份不会被揭示的实体,在本部分中,一个声称方按 ISO/IEC 20008-2 规定的群组签名方案充当一个签名方的角色;

注:在一些机制中,声称方的角色在多个实体之间分解。例如,直接匿名验证(DAA)机制就涉及一个具有有限计算和存储能力的主要声称方,比如一个可信平台模块(TPM),以及一个具有更高计算能力但更低安全容错性的辅助声称方,比如一个普通计算机平台(即内嵌 TPM 的主机)。

——验证方(Verifier):一个验证声称方身份正确性的实体,而其并不知道声称方的真实身份;

——发布方(Issuer):一个给声称方分发群组成员凭证的实体,该实体存在于 ISO/IEC 20008-2 规定的所有机制中;

——打开方(Opener):一个能够确定使用在鉴别过程中产生的群组签名的声称方身份的实体,该实体存在于 ISO/IEC 20008-2 规定的部分机制中。在某些机制,群组成员关系发布方、群组成员打开方是相同的实体;

——连接方(Linker):一个能够判断用于鉴别的两个群组签名是否来源于同一个声称方的实体。该实体存在于 ISO/IEC 20008-2 规定的部分机制中。在一些机制中,这个连接方也是验证方,在一个匿名实体验证的机制中,这些连接方的数量是不固定的。

要求每个参与匿名实体鉴别机制的实体都知道一个公共的群组参数,这个参数用于该机制中的许多函数的计算。

GB/T 34953 的本部分规定的 24 种验证机制有如下预期用途。如果在线 TTP 不是必要的或是不可用的,宜使用第 7 章的机制。在第 7 章的 16 种机制中,第 1～第 8 种机制没有绑定属性,而第 9～第 16 种机制则具有绑定属性。如果需要使用在线 *TTP* 参与的机制,则宜使用第 8 章中的机制。第 7 章和第 8 章规定的机制都提供单向匿名鉴别、双向匿名鉴别和单向匿名双向鉴别,并根据不同的步数提供多种选项。本部分所规定的各机制的对象标识符见附录 A。

撤销过程用于撤销用户并且检查用户是否被撤销,这个过程的细节依赖于用于产生匿名鉴别的权标(*Token*)的匿名数字签名方案。ISO/IEC 20008-1 规定了撤销过程的一般模型,ISO/IEC 20008-2 规定了使用一个群组公钥的个人匿名签名方案的操作过程。

6 密钥产生过程

密钥产生过程包含生成群组成员分发密钥、群组成员打开密钥和在机制有要求时的群组签名连接

密钥(或多个密钥)的密钥产生算法。密钥产生算法的细节在本部分的范围之外。

密钥产生过程也包含了一个群组成员的发布过程,该群组成员发布过程在一个群组成员和一个发布方之间操作,且涉及一个群组成员签名密钥的创建。

为了防止窃听者观察到群组成员的凭证以及确保群组成员凭证只提供给一个合法的群组成员,一个群组成员(作为声称方)和一个发布方之间要求一个安全可靠的信道。本部分并没有规定群组发布方如何验证一个群组成员。

密钥产生包括步骤 a)和步骤 b),如图 1 所示,详细步骤如下:

a) 群组成员发布方将群组发布密钥、群组公钥、群组公共参数以及可选的可区分标识符作为输入。在这一步,一个群组成员发布方可以和一个群组成员交互操作;

b) 群组成员发布过程输出一个群组成员签名密钥。

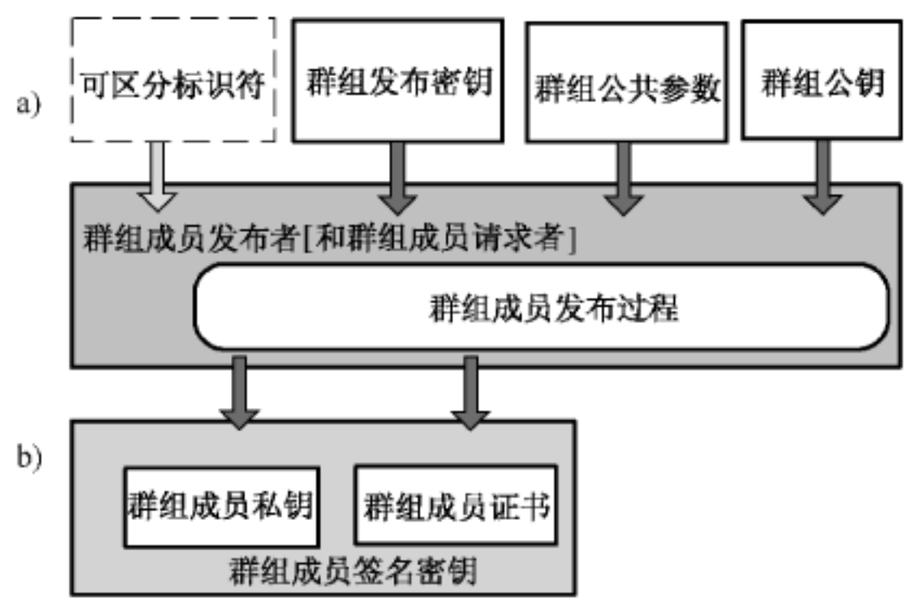

图 1 群组成员的发布过程

7 无在线可信第三方参与的匿名鉴别机制

7.1 概述

本章给出了无在线可信第三方参与的匿名实体鉴别机制。本章中规定的机制使用群组公钥证书或者其他手段验证群组公钥的有效性。这些机制用于覆盖打开和连接过程的扩展分别在第 9 章和第 10 章中规定。

指定的实体鉴别机制使用时变参数如时间戳,序列号或随机数(参见 ISO/IEC 9798-1:2010[3]的附录 B)。

在本部分中,权标可采用如下形式:

$Token = X_1 \| X_2 \| \ldots X_j \| gsS_{XA}(Y_1 \| Y_2 \ldots \| Y_j)$。

在一个单向匿名双向鉴别机制中,一个数字签名 $sS_X(Y_1 \| Y_2 \ldots \| Y_j)$可被一个群组签名 $sS_{XG}(Y_1 \| Y_2 \ldots \| Y_j)$代替。

在带有绑定特性的双向匿名鉴别机制和带有绑定特性的单向匿名双向鉴别机制中,MAC 可另外级联或者 MAC 可取代群组签名 $sS_{XG}(Y_1 \| Y_2 \ldots \| Y_j)$。

在本部分中,“被签名消息”指的是被用作群组签名方案的输入的数据串 $Y_1 \| Y_2 \ldots \| Y_j$。“消息”指的是数据串 $X_1 \| X_2 \| \ldots X_j$。$X_1 \| X_2 \| \ldots X_j$ 和 $Y_1 \| Y_2 \ldots \| Y_j$ 的关键部分宜保持相同,其他部分因它们采用的群组签名方案和特定的应用而可能有所不同。

如果包含在权标中被签名消息里的信息能够从群组签名中恢复,则它不必被包含在权标的信息中。

如果包含在权标中被签名消息里的文本部分不能够从群组签名中被恢复,则它应被包含在权标的非签名信息中。

如果在权标中被签名消息的信息是由声称方发送到验证方,且验证方已经知晓这个信息(例如一个

随机数),则它不必包含在权标的信息中。

在本部分规定的机制中所规定的所有文本字段都是可以使用的,但具体如何使用不在本部分的规定范围之内,这些文本字段之间的关系和内容取决于特定的应用。关于文本字段的使用相关的信息参见 ISO/IEC 9798-3[4]的附录 A。

注 1:第一个实体在其签名的数据块中包括它自己的随机数,可以减轻当该数据块已经被恶意的第二个实体所控制时的、与数据块实体签名相关的安全问题。在这种情况下,随机数的不可预测性防止了完全预定义数据的签名。

注 2:群组公钥证书的分配超出了本部分的标准化范围,除了涉及第 8 章规定的在线可信第三方参与的鉴别机制外,群公钥证书的发送在所有机制中都是可选的。

7.2 描述了单向匿名鉴别机制,这种机制为一个实体提供对端实体的合法性确认,反之亦然。7.3 描述了双向匿名鉴别机制,这种机制为两个实体相互间提供合法性确认。7.4 描述了单向匿名双向鉴别机制,在一个方向上提供匿名实体鉴别,另一个方向上提供实体鉴别。

7.3 和 7.4 中规定的三次传递鉴别协议和两次传递并行的鉴别协议可能会遭受到"误绑定"攻击(参见参考文献[11]),当质询和权标信息没有被绑定到一起,将有可能出现一个实体去发送质询信息后而在相同群组中的另外一个实体假冒前一个实体发送权标信息的情况。关于误绑定攻击以及绑定属性的更多信息参见附录 B。

为减弱误绑定攻击,7.5 和 7.6 规定了八种具有绑定属性的用于两次传递和三次传递并行的鉴别协议的机制。

7.2 单向匿名鉴别

7.2.1 总则

单向匿名鉴别是指两实体中只有一个实体(即声称方,群组 G 中的实体 A)被鉴别,而被鉴别实体对于对端实体(即验证方 B)是匿名的。

7.2.2 机制 1——一次传递单向匿名鉴别

该机制由群组 G 中的实体 A 向实体 B 发起鉴别协议。惟一性或时效性通过产生并检查时间戳或序列号(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。

该鉴别机制如图 2 所示,由实体 A 发起,实体 B 完成对实体 A 的鉴别。

图 2 一次传递单向匿名鉴别

声称方 A 发送给验证方 B 的权标 $Token_{AB}$ 形式为:

$$Token_{AB} = T_A(\text{或 } N_A) \parallel B \parallel [Text_2] \parallel gsS_{GA}(T_A(\text{或 } N_A) \parallel B \parallel [Text_1])。$$

声称方 A 选用时间戳 T_A 或序列号 N_A 为时变参数,该选择依赖于声称方的技术能力和验证方的环境。签名值 gsS_{AG} 是群组签名,使用了 ISO/IEC 20008-2 中描述的群组签名机制。$Cert_G$ 是群组公钥证书,该证书包含群组 G 的群组公钥。

注 1:权标 $Token_{AB}$ 的被签名消息中包含标识符 B 是必要的,可以防止权标被除了指定的验证方以外的验证方所接收。

注 2:通常,该过程不验证 $Text_2$。

注 3:本机制的一种应用是密钥分发(参见 ISO/IEC 9798-1:2010[3]的附录 A)。

本机制执行过程如下：

a) A 发送 $Token_{AB}$ 和可选证书字段 $Cert_G$ 给 B。

b) 收到包含 $Token_{AB}$ 的消息后，B 执行下列步骤：

1) 通过验证 G 的群组公钥证书或者其他方式获得群组 G 的有效群组公钥；

2) 通过下列方式校验 $Token_{AB}$：验证 $Token_{AB}$ 中 A 的群组签名，检查时间戳或者序列号，检查 $Token_{AB}$ 中被签名消息中的标识符域的值(B)与 B 的可区分标识符是否一致。

7.2.3 机制 2——两次传递单向匿名鉴别

该鉴别机制由实体 B 发起，完成对实体 A 的鉴别，如图 3 所示。惟一性或时效性通过产生并检查随机数 R_B(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。

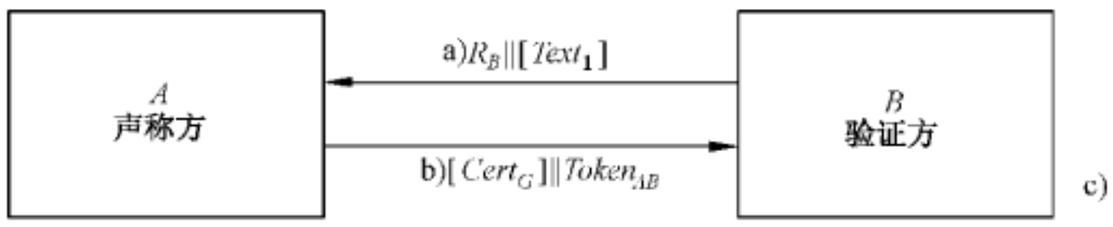

图 3 两次传递单向匿名鉴别

声称方 A 发送给验证方 B 的权标 $Token_{AB}$ 的形式如下：

$Token_{AB} = R_A \| R_B \| [B] \| Text_3 \| gsS_{GA}(R_A \| R_B \| [B] \| [Text_2])$。

其中 B 的标识符是可选的，依赖于鉴别机制的应用环境。

注 1：$Token_{AB}$ 的待签名消息中包含可选的标识符 B，用于防止权标被预期的验证方之外的恶意验证方接收(例如，可能出现在中间人攻击中)。

注 2：$Token_{AB}$ 的签名部分包含随机数 R_A，用于防止 B 在鉴别机制开始之前获得 A 对 B 所选数据的群组签名。当实体 A 在实体鉴别机制之外使用相同的群组公钥或者其他群组成员使用该群组公钥时，该措施是必要的。

本机制执行过程如下：

a) B 发送随机数 R_B 和可选文本字段 $Text_1$ 到 A。

b) A 发送 $Token_{AB}$ 和可选证书字段 $Cert_G$ 到 B。

c) 收到包含 $Token_{AB}$ 的消息后，B 执行下列步骤：

1) 通过验证群组 G 的公钥证书或者其他方式获得群组 G 的有效群组公钥；

2) 通过下列方式校验 $Token_{AB}$：验证 $Token_{AB}$ 中 A 的群组签名，检查步骤 a)中的随机数 R_B 与 $Token_{AB}$ 中被签名消息里的 R_B 是否一致，检查 $Token_{AB}$ 中被签名消息中的标识符域的值(B)与 B 的可区分标识符是否一致。

7.3 双向匿名鉴别

7.3.1 总则

双向匿名鉴别是指两个通信实体互相鉴别，并且两个实体互相间都是匿名的。

7.2.2 和 7.2.3 中规定的两项机制，在 7.3.2 和 7.3.3 中通过发送一条额外的消息的方式分别进行了扩展，以实现双向鉴别。

7.3.4 中规定的机制使用四次传递，但不必所有消息都连续发送。因此，执行该鉴别过程所用的时间有可能减少。

7.3.2 机制 3——两次传递双向匿名鉴别

该鉴别机制由群组 G 中的实体 A 向群组 G' 中的实体 B 发起鉴别协议，如图 4 所示。惟一性或时效性通过产生并检查时间戳或序列号(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。实体 A 知道

群组G'的身份。

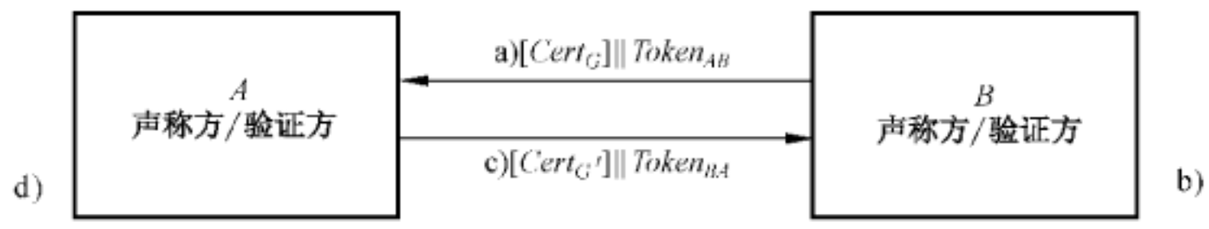

图 4　两次传递双向匿名鉴别

实体 A 发送给实体 B 的权标 $Token_{AB}$ 形式为：

$Token_{AB}=T_A$(或 N_A)‖G'‖[$Text_2$]‖gsS_{GA}(T_A(或 N_A)‖G'‖[$Text_1$])。

实体 B 发送给实体 A 的权标 $Token_{BA}$ 形式为：

$Token_{BA}=T_B$(或 N_B)‖G‖[$Text_4$]‖$gsS_{BG'}$(T_B(或 N_B)‖G‖[$Text_3$])。

在本机制中选择使用时间戳或序列号依赖于声称方的能力以及验证方的环境。

注 1：$Token_{AB}$ 和 $Token_{BA}$ 中被签名消息中分别包含标识符 G 和 G' 是必要的，它用于防止权标被恶意群组中的成员所接收。

本机制执行过程如下：

a)　A 发送 $Token_{AB}$ 和可选证书字段 $Cert_G$ 到 B；

b)　收到包含 $Token_{AB}$ 的消息后，B 执行下列步骤：

　1)　通过验证群组 G 的公钥证书或其他方式获得群组 G 的有效群组公钥；

　2)　通过以下方式来校验 $Token_{AB}$：验证 $Token_{AB}$ 中 A 的群组签名，检查时间戳或者序列号，检查 $Token_{AB}$ 中被签名消息中的标识符域的值(G')与 G' 的可区分标识符是否一致。

c)　B 发送 $Token_{BA}$ 和可选证书字段 $Gert_{G'}$ 给 A。

d)　收到包含 $Token_{BA}$ 的消息，A 执行如下步骤：

　1)　通过验证群组 G' 的公钥证书或其他方式获得群组 G' 的有效群组公钥；

　2)　通过下列方式校验 $Token_{BA}$：验证包含在 $Token_{BA}$ 中的 B 的签名，检查时间戳或者序列号，检查 $Token_{AB}$ 中被签名消息中的标识符域的值(G)与 G 的可区分标识符是否一致。

注 2：该机制的两个消息不以任何方式联系在一起，除了隐含的实时性；该机制包含了两个独立的、在 7.2.2 中所规定机制的少量修改版本的使用。这些信息的进一步绑定可以通过适当使用文本字段来实现。

7.3.3　机制 4——三次传递双向匿名鉴别

该鉴别机制由群组 G' 中的实体 B 发起鉴别协议，实体 A 在群组 G 中，如图 5 所示。惟一性或时效性通过产生并检查时间戳或序列号(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。

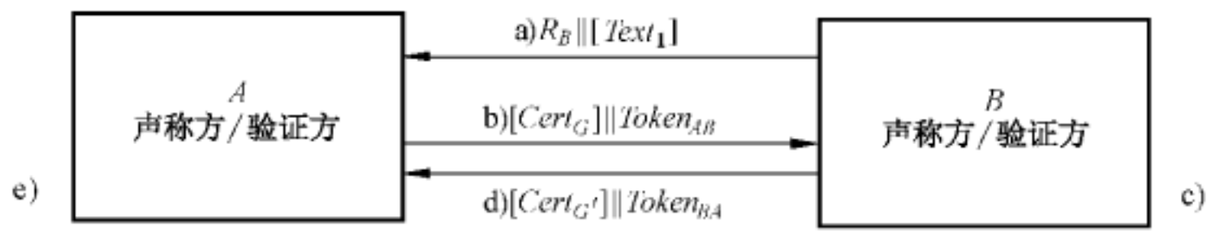

图 5　三次传递双向匿名鉴别

权标形式如下：

$Token_{AB}=R_A$‖R_B‖[G']‖$Text_3$‖gsS_{AG}(R_A‖R_B‖[G']‖[$Text_2$])；

$Token_{BA}=R_B$‖R_A‖[G]‖$Text_5$‖$gsS_{AG'}$(R_B‖R_A‖[G]‖[$Text_4$])。

注 1：$Token_{AB}$ 里的被签名消息中包含随机数 R_A，用于防止 B 在鉴别机制开始之前获得 A 对 B 所选数据的群组签名。当实体 A 在实体鉴别机制之外使用相同的群组公钥或者其他群组成员使用该群组公钥时，这个措施是必要的。但是基于安全考虑，$Token_{BA}$ 里包括 R_B 是必要的。A 宜检查其是否与第一个消息中的 R_B 值一致。但可能不会给 B 提供相同的保护，因为在 R_A 被选择前 A 已经知晓 R_B。为了实现相同的保护水平，B 可以在

$Token_{BA}$ 里的 $Text_4$ 和 $Text_5$ 中插入另一个随机数 R'_B。

注 2：包含在 $Token_{AB}$ 中的标识符 G' 和 $Token_{BA}$ 中的标识符 G 是可选的。包含这些标识符的需求依赖于鉴别机制被使用的环境。

本机制执行过程如下：

a) B 发送随机数 R_B 和可选文本字段 $Text_1$ 到 A。

b) A 发送 $Token_{AB}$ 和可选证书字段 $Cert_G$ 到 B。

c) 收到包含 $Token_{AB}$ 的消息后，B 执行下列步骤：

   1) 通过验证群组 G 的公钥证书或其他方式获得群组 G 的有效群组公钥。

   2) 通过下列方式校验 $Token_{AB}$：验证包含在 $Token_{AB}$ 中的 A 的群组签名，检查在步骤 a)中发送给 A 的随机数 R_B 与包含在 $Token_{AB}$ 中被签名消息中的随机数 R_B 是否一致，检查 $Token_{AB}$ 中被签名消息中的标识符域的值(G')与 G' 的可区分标识符是否一致。

d) B 发送 $Token_{BA}$ 和可选证书字段 $Cert_{G'}$ 到 A。

e) 收到包含 $Token_{BA}$ 的消息后，A 执行类似于步骤 c)中的 1)和 2)的步骤。此外，A 检查包含在 $Token_{BA}$ 中被签名消息中的随机数 R_B 与在步骤 a)收到的随机数 R_B 是否一致，检查包含在 $Token_{BA}$ 中被签名消息中的随机数 R_A 与在步骤 b)发送的随机数 R_A 是否一致。

7.3.4 机制 5——两次传递并行的双向匿名鉴别

该鉴别机制中群组 G 中的实体 A 与群组 G' 中的实体 B 并行的鉴别，如图 6 所示。惟一性或时效性通过产生并检查随机数(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。

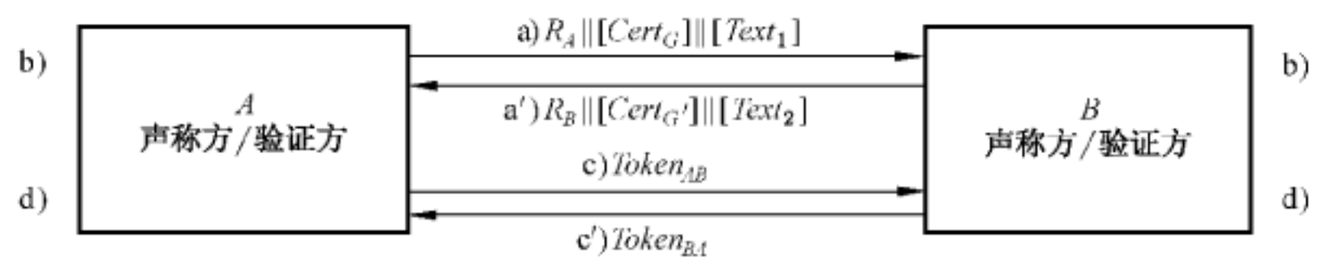

图 6 两次传递并行的双向匿名鉴别

本机制中产生的权标如下：

$Token_{AB} = R_A \| R_B \| [G'] \| Text_4 \| gsS_{AG}(R_A \| R_B \| [G'] \| [Text_3])$；

$Token_{BA} = R_B \| R_A \| [G] \| Text_6 \| gsS_{AG'}(R_B \| R_A \| [G] \| [Text_5])$。

$Token_{AB}$ 中的标识符 G' 和 $Token_{BA}$ 中的标识符 G 是可选的。是否包含这些标识符依赖于使用该鉴别机制的环境。

注 1：$Token_{AB}$ 里的随机数 R_A，用于防止 B 在鉴别机制开始之前获得 A 对 B 所选数据的群组签名。当实体 A 在实体鉴别机制之外使用相同的群组公钥或者其他群组成员使用该群组公钥时，这个措施是必要的。出于相同的原因，$Token_{BA}$ 里包括 R_B 也是必要的。通过接收步骤 a)和 a′)所发消息的相对时间，一方实体在选择自己随机数的时候，可能已经获得了对方的随机数。为了解决上述问题，两个实体可分别在 $Token_{AB}$ 中的文本字段 $Text_3$ 和 $Text_4$，$Token_{BA}$ 里的文本字段 $Text_5$ 和 $Text_6$ 插入 R_A' 和 R'_B。

机制执行如下步骤：

a) A 发送随机数 R_A，可选证书字段 $Cert_G$ 和可选文本字段 $Text_1$ 到 B；

a′) B 发送随机数 R_B，可选证书字段 $Cert_{G'}$ 和可选文本字段 $Text_2$ 到 A；

b) A 和 B 通过验证群组公钥证书或其他方式获得对端实体所在群组的有效群组公钥；

c) A 发送 $Token_{AB}$ 到 B；

c′) B 发送 $Token_{BA}$ 到 A；

d) A 和 B 执行下列步骤：每个实体通过下列方式校验接收到的权标：验证包含在权标中的群组签名，检查已发送到对端实体的随机数与包含在接收到的权标中的被签名消息中的随机数是

否一致。

注 2:双向运行 7.2.3 定义的机制两次可以达到与 7.3.4 机制相同的功能。在 7.3.4 机制里第一个消息里就包括群组公钥证书允许群组公钥证书校验在早期进行,这样就加快了鉴别处理的速度。

注 3:这种机制的两个消息并不以任何方式联系在一起,除了隐含的实时性。

7.4 单向匿名双向鉴别

7.4.1 总则

单向匿名双向鉴别是指两个通信实体双向鉴别对端身份,但是其中仅一个实体对另外一个实体采用的是匿名鉴别。

在本机制中,群组 G 中的实体 A 被实体 B 采用 ISO/IEC 20008-2 中规范的群组数字签名机制进行匿名鉴别,而实体 B 被群组 G 中的实体 A 采用 ISO/IEC 14888-3 或 ISO/IEC 9796[2]中规范的数字签名机制进行鉴别。

7.4.2 机制 6——两次传递单向匿名双向鉴别

该鉴别机制由群组 G 中的实体 A 向实体 B 发起鉴别,如图 7 所示。惟一性或时效性通过产生并检查时间戳或序列号(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。

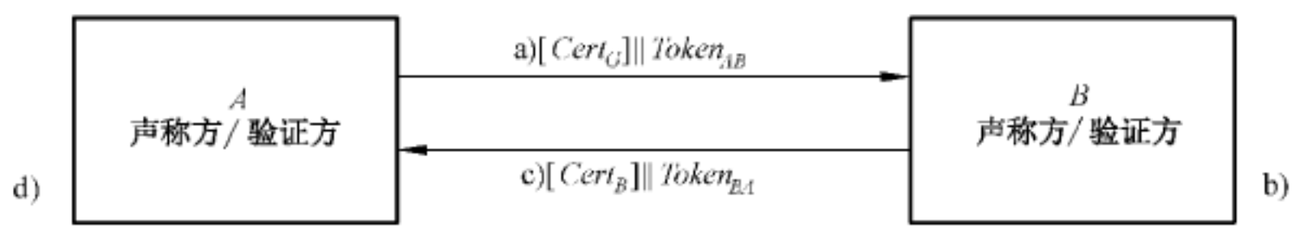

图 7 两次传递单向匿名双向鉴别

权标 $Token_{AB}$ 的形式如下:

$Token_{AB}=T_A$(或 N_A)‖B‖[$Text_2$]‖gsS_{GA}(T_A(或 N_A)‖B‖[$Text_1$])。

权标 $Token_{BA}$ 的形式如下:

$Token_{BA}=T_B$(或 N_B)‖G‖[$Text_4$]‖sS_B(T_B(或 N_B)‖G‖[$Text_3$])。

本机制中使用随机数或时间戳来保证惟一性或时效性依赖于鉴别者的鉴别能力和验证者的鉴别环境。

注 1:$Token_{BA}$ 和的被签名消息中分别包含标识符 G 和 B,用以防止权标被恶意的验证方接收。

本机制执行过程如下:

a) A 发送 $Token_{AB}$ 和可选证书字段 $Cert_G$ 到 B。

b) 收到包含权标 $Token_{AB}$ 的消息后,B 执行下列步骤:

   1) 通过验证群组 G 的公钥证书或其他方式获得群组 G 的有效群组公钥。

   2) 通过下列方式校验 $Token_{AB}$:验证包含在 $Token_{AB}$ 中的 A 的群组签名,检查时间戳或者序列号,检查 $Token_{AB}$ 中被签名消息中的标识符域的值(B)与 B 的可区分标识符是否一致。

c) B 发送权标 $Token_{BA}$ 和可选证书字段 $Cert_B$ 到 A。

d) 收到包含权标 $Token_{BA}$ 的消息后,A 执行下列步骤:

   1) 通过验证 B 的证书或其他方式获得 B 的有效公钥;

   2) 通过下列方式校验 $Token_{BA}$:验证包含在权标中的 B 的签名,检查时间戳或者序列号,检查 $Token_{BA}$ 中被签名消息中的标识符域的值(G)与 G 的可区分标识符是否一致。

注 2:这种机制的两个消息并不以任何方式联系在一起,除了隐含的实时性;该机制包含了两个独立的、在 7.2.2 中所规定机制的少量修改版本的使用。这些信息的进一步绑定可以通过适当使用文本字段来实现。

7.4.3 机制 7——三次传递单向匿名双向鉴别

该鉴别机制中由群组 G 中的实体 A 向实体 B 发起鉴别，如图 8 所示。惟一性或时效性通过产生并检查时间戳或序列号(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。

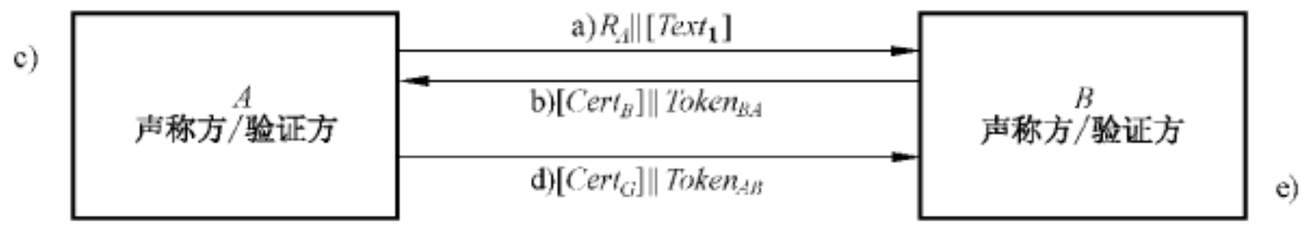

图 8 三次传递单向匿名双向鉴别

权标形式如下：

$Token_{BA} = R_B \| R_A \| [G] \| Text_3 \| sS_B(R_B \| R_A \| [G] \| [Text_2])$；

$Token_{AB} = R_A \| R_B \| [B] \| Text_5 \| gsS_{AG}(R_A \| R_B \| [B] \| [Text_4])$。

$Token_{BA}$ 和 $Token_{AB}$ 中各自包含可选的 G 和 B 的可区分标识符，是否包括这些标识符取决于鉴别机制使用的环境。

注：$Token_{BA}$ 里的被签名消息里包含随机数 R_B，用于防止 A 在鉴别机制开始之前获得 A 对 B 所选数据的群组签名。当实体 A 在实体鉴别机制之外使用相同的群组公钥或者其他群组成员使用该群组公钥时，这个措施是必要的。但是基于安全原因，$Token_{AB}$ 里包括 R_A 也是必要的。B 宜检查其是否与第一个消息里的 R_A 值一致。但可能不会给 A 提供相同的保护，因为在 R_A 被选择前 A 已经知晓 R_B。为了实现相同的保护水平，A 可以在 $Token_{AB}$ 里的 $Text_2$ 和 $Text_3$ 里插入另一个随机数 R_A'。

本机制执行过程如下：

a) A 发送随机数 R_A 和可选文本字段 $Text_1$ 到 B。

b) B 发送 $Token_{BA}$ 和可选证书字段 $Cert_B$ 到 A。

c) 收到包含 $Token_{BA}$ 的消息后，A 执行下列步骤：

   1) 通过验证 B 的公钥证书或其他方式获得 B 的有效公钥；

   2) 通过下列方式校验 $Token_{BA}$：验证包含在 $Token_{BA}$ 中的 B 的签名，检查在步骤 a)中发送到 A 的随机数 R_A 与包含在 $Token_{BA}$ 中被签名消息中的随机数 R_A 是否一致，如果 $Token_{BA}$ 的被签名消息中包含 G 的标识符字段，则检查其值与 G 的可区分标识符是否一致。

d) A 发送 $Token_{AB}$ 和它的群组公钥证书(可选)给 B。

e) 接收到包含 $Token_{AB}$ 的消息后，B 执行下列步骤：

   1) 通过验证 G 的公钥证书 $Cert_G$ 或其他方式获得群组 G 的有效群组公钥；

   2) 通过下列方式校验 $Token_{AB}$：验证包含在 $Token_{AB}$ 中的 A 的群组签名，检查包含在 $Token_{AB}$ 中被签名消息中的 R_A 与在步骤 a)中收到的随机数 R_A 是否一致，检查包含在 $Token_{AB}$ 被签名消息中的 R_B 与在步骤 b)中发送的随机数 R_B 是否一致，如果 $Token_{AB}$ 的被签名消息中包含 B 的标识符字段，则检查其值与 B 的可区分标识符是否一致。

7.4.4 机制 8——两次传递并行的单向匿名双向鉴别

该匿名鉴别机制被并行的执行于属于群组 G 的实体 A 和实体 B 之间，如图 9 所示。惟一性或时效性通过产生并检查随机数(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。

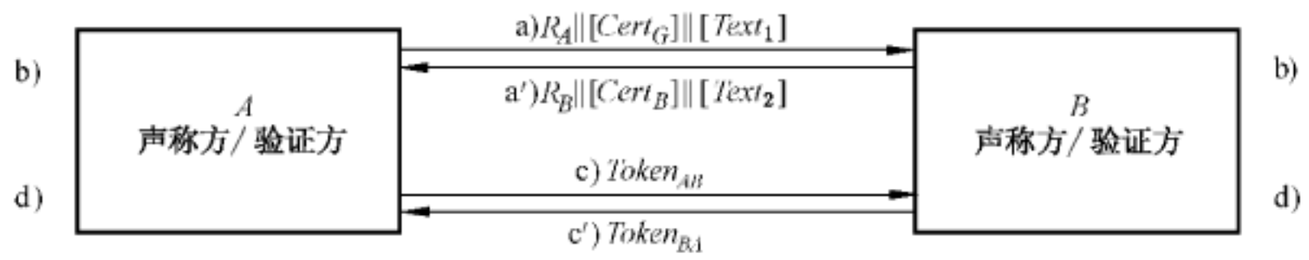

图 9　两次传递并行的单向匿名双向鉴别

权标形式如下：

$Token_{AB} = R_A \| R_B \| [B] \| Text_4 \| gsS_{AG}(R_A \| R_B \| [B] \| [Text_3])$；

$Token_{BA} = R_B \| R_A \| [G] \| Text_6 \| sS_B(R_B \| R_A \| [G] \| [Text_5])$。

$Token_{AB}$ 中的标识符 B 和 $Token_{BA}$ 中的标识符 G 是可选的。是否包含这些标识符依赖于使用该鉴别机制的环境。

注：$Token_{AB}$ 里的随机数 R_A，用于防止 B 在鉴别机制开始之前获得 A 对 B 所选数据的群组签名。当实体 A 在实体鉴别机制之外使用相同的群组公钥或者其他群组成员使用该群组公钥时，这个措施是必要的。但基于安全原因，$Token_{BA}$ 里包括 R_B 也是必要的。通过步骤 a)和 a′)消息接收的相对时间，一方实体在选择自己随机数的时候，可能已经获得了对方的随机数。为了解决上述问题，两个实体分别在 $Token_{AB}$ 里的文本字段 $Text_3$ 和 $Text_4$，$Token_{BA}$ 里的文本字段 $Text_5$ 和 $Text_6$ 插入 R'_A 和 R'_B。

本机制的执行过程如下：

a)　A 发送随机数 R_A，可选证书字段 $Cert_G$ 和可选文本字段 $Text_1$ 到 B。

a′)　B 发送随机数 R_B，可选证书字段 $Cert_B$ 和可选文本字段 $Text_2$ 到 A。

b)　A 通过验证 B 的证书 $Cert_B$ 或其他方式获得 B 的有效公钥。类似，B 通过验证 A 所属群组 G 的公钥证书 $Cert_G$ 或其他方式获得群组 G 的有效群组公钥。

c)　A 发送权标 $Token_{AB}$ 到 B。

c′)　B 发送权标 $Token_{BA}$ 到 A。

d)　A 和 B 各自通过下列方式校验权标：验证包含在各自接收到的权标中的签名或群组签名，检查权标中被签名消息中的随机数与已发送到对方实体的随机数是否一致。

7.5　带有绑定特性的双向匿名鉴别

7.5.1　总则

带有绑定特性的双向匿名鉴别是指两个实体双向鉴别，但是对于鉴别方来说，被鉴别方的真实身份是不被透漏的，绑定特性用于提供这种保证。

本节规定了带有绑定特性的双向匿名实体机制的细节。这些机制中，群组 G 中的实体 A 与群组 G' 中的实体 B 应使用 ISO/IEC 20008-2 规定的群签名机制进行鉴别。

注：7.5 描述的机制里，实体 A 和实体 B 可选择从一个共享密钥导出一个会话密钥，用于保护实体间通信的安全。会话密钥的导出及使用超出本部分范围。

7.5.2　机制 9——三次传递签名在后双向匿名鉴别

该带有绑定特性的三次传递匿名鉴别协议中，实体发送的第一条消息不包含群组签名，由群组 G' 中的实体 B 向群组 G 中的实体 A 发起鉴别。惟一性或时效性通过产生并检查随机数(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。协议如图 5 所示。

本机制应满足下列要求：

——考虑到 DDH 难解问题，实体 A 和实体 B 一定要协商 q 阶的循环群 G 及循环群 G 的生成元。

协议消息及所需的其他信息描述如下：

临时公钥 $R_B = g^b$，在 Z_q 中对应临时私钥 b；

临时公钥 $R_A=g^a$，在 Z_q 中对应临时私钥 a。

权标形式如下：

$Token_{AB}=R_A \| Text_3 \| gsS_{AG}(R_A \| R_B \| [Text_2]) \| MAC_{AB})$；

$Token_{BA}=R_B \| Text_5 \| gsS_{BG}(R_B \| R_A \| [Text_4]) \| MAC_{BA})$。

其中：

$MAC_{AB}=mac_{MK}([Cert_G] \| R_A \| [Text_3] \| gsS_{AG}(R_A \| R_B \| [Text_2]))$；

$MAC_{BA}=mac_{MK}([Cert_{G'}] \| R_B \| [Text_5] \| gsS_{BG'}(R_B \| R_A \| [Text_4]))$。

本机制执行过程如下：

a) B 执行下列步骤：

1) 从 Z_q 中选择临时私钥 b，计算临时公钥 $R_B=g^b$；

2) 发送 g^b 和可选文本字段 $Text_1$ 到 A。

b) A 执行下列步骤：

1) 从 Z_q 中选择临时私钥 a，计算临时公钥 $R_A=g^a$；

2) 计算 $g^{ab}=(R_B)^a$；

3) 计算 MAC 密钥 $MK=kgf(g^{ab})$；

4) 用签名密钥计算 $gsS_{AG}=(R_A \| R_B \| Text_2)$；

5) 用 MAC 密钥 MK 计算：

$MAC_{AB}=mac_{MK}([Cert_G] \| R_A \| [Text_3] \| gsS_{AG}(R_A \| R_B \| [Text_2]))$；

6) 发送 $Token_{AB}$ 和可选证书字段 $Cert_G$ 到 B。

c) 收到包含 $Token_{AB}$ 的消息后，B 执行下列操作：

1) 计算 $g^{ab}=(R_A)^b$。

2) 计算 MAC 密钥 $MK=kgf(g^{ab})$。

3) 通过验证群组 G 的群组公钥证书或者其他方式来获得群组 G 的公钥。

4) 通过下列方式校验 $Token_{AB}$：

i) 校验包含在 $Token_{AB}$ 中的 A 的签名；

ii) 检查包含在群组签名中的临时公钥 R_A 和 R_B；

iii) 检查包含在 $Token_{AB}$ 中的临时公钥 R_B 是否等于在步骤 a)中发送的临时公钥 R_B；

iv) 用 MK 验证 MAC_{AB} 的值。

5) 用签名密钥计算 $gsS_{BG'}=(R_B \| R_A \| Text_4)$。

6) 用 MAC 密钥 MK 计算：

$MAC_{BA}=mac_{MK}([Cert_{G'}] \| R_B \| [Text_5] \| gsS_{BG'}(R_B \| R_A \| [Text_4]))$。

d) B 发送权标 $Token_{BA}$ 和可选证书字段 $Cert_{G'}$ 到 A。

e) 收到包含权标 $Token_{BA}$ 的消息后，A 执行下列步骤：

1) 通过验证群组 G' 的群组公钥证书或其他方式来获得群组 G' 的有效公钥。

2) 通过下列方式校验 $Token_{BA}$：

i) 校验包含在 $Token_{BA}$ 中的 B 的签名；

ii) 检查包含在群组签名中的临时公钥 R_B 和 R_A；

iii) 检查包含在 $Token_{BA}$ 中的临时公钥 R_B 与在步骤 a)中收到的临时公钥 R_B 是否一致；

iv) 检查包含在权标 $Token_{AB}$ 中的群组签名中的临时公钥 R_A 与在步骤 b)中发送的临时公钥 R_A 是否一致；

v) 用 MK 验证 MAC_{BA} 的值。

7.5.3 机制 10——三次传递签名在先双向匿名鉴别

该带有绑定特性的三次传递匿名鉴别协议中，实体发送的第一条消息包含群组签名，由群组 G' 中的实体 B 向群组 G 中的实体 A 发起鉴别，如图 10 所示。惟一性或时效性通过产生并检查随机数(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。

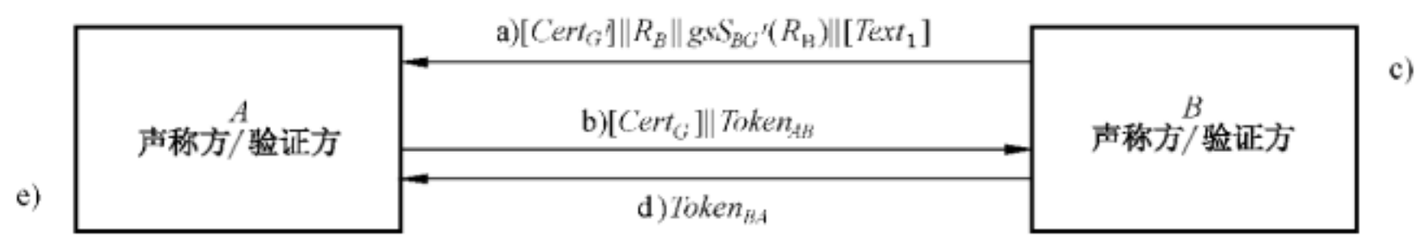

图 10 三次传递签名在先双向匿名鉴别

在执行本机制时，应满足下列要求：

——考虑到 DDH 难解问题，实体 A 和实体 B 一定要协商 q 阶的循环群 G 及循环群 G 的生成元。

协议消息及所需的其他信息描述如下：

临时公钥 $R_B=g^b$，在 Z_q 中对应临时私钥 b；

临时公钥 $R_A=g^a$，在 Z_q 中对应临时私钥 a。

权标形式如下：

$Token_{AB}=R_A \parallel gsS_{AG}(R_A) \parallel MAC_{AB} \parallel [Text_2]$；

$Token_{BA}=MAC_{BA} \parallel [Text_3]$。

其中：

$MAC_{AB}=mac_{MK}(R_A \parallel gsS_{AG}(R_A) \parallel R_B \parallel gsS_{BG'}(R_B) \parallel [Text_4])$；

$MAC_{BA}=mac_{MK}(R_B \parallel gsS_{BG'}(R_B) \parallel R_A \parallel gsS_{AG}(R_A) \parallel [Text_5])$。

本机制执行过程如下：

a) B 执行下列步骤：

1) 从 Z_q 中选择临时私钥 b，计算临时公钥 $R_B=g^b$；

2) 使用签名密钥计算 $gsS_{BG'}(R_B)$；

3) 发送 g^b、$gsS_{BG'}(R_B)$、可选证书字段 $Cert_{G'}$ 和可选文本字段 $Text_1$ 到 A。

b) A 执行下列步骤：

1) 通过验证群组 G' 的群组公钥证书或其他方式获得群组 G' 的有效公钥；

2) 验证 B 的群组签名；

3) 从 Z_q 中选择临时私钥 a，计算临时公钥 $R_A=g^a$；

4) 用签名密钥计算 $gsS_{AG}(R_A)$；

5) 计算 $g^{ab}=(R_B)^a$；

6) 计算 MAC 密钥 $MK=kgf(g^{ab})$；

7) 用 MAC 密钥 MK 计算：

$MAC_{AB}=mac_{MK}(R_A \parallel gsS_{AG}(R_A) \parallel R_B \parallel gsS_{BG}(R_B) \parallel [Text_4])$；

8) 发送 $Token_{AB}$ 和可选证书字段 $Cert_G$ 到 B。

c) 收到包含 $Token_{AB}$ 的消息后，B 执行下列步骤：

1) 通过验证群组 G 的群组公钥证书或其他方式获得群组 G 的有效公钥；

2) 验证 A 的群组签名；

3) 计算 $g^{ab}=(R_A)^b$；

4) 计算 MAC 密钥 $MK=kgf(g^{ab})$；

5) 用 MAC 密钥 MK 计算：

$MAC_{BA}=mac_{MK}(R_B \| gsS_{BG'}(R_B) \| R_A \| gsS_{AG}(R_A) \| [Text_5])$；

6） 用 MK 验证 MAC_{AB} 的值。

d） B 发送 $Token_{BA}$ 到 A。

e） 收到包含 $Token_{BA}$ 的消息后，A 用 MK 检查 MAC_{BA} 的值。

注：在上述机制里，为了提供更健壮的绑定特性，可将 MAC 改为支持用户可控的连接能力的群组签名，如 DAA。更健壮的绑定特性（也称之为完全绑定特性）保证了所有接收到的消息都来自相同的声称方（详细描述参考第10章）。本注同样适用于7.5.5、7.6.3和7.6.5描述的机制。

7.5.4 机制11——两次传递并行的签名在后双向鉴别

该带有绑定特性的两次传递并行的签名在后的双向鉴别协议中，实体发送的第一条消息不包含群组签名，匿名鉴别过程在由群组 G' 中的实体 A 和群组 G' 中的实体 B 执行。惟一性或时效性通过产生并检查随机数（参见ISO/IEC 9798-1:2010[3]的附录B）来控制。协议如图6所示。

在执行本机制时，应满足下列要求：

——考虑到DDH难解问题，实体 A 和实体 B 一定要协商 q 阶的循环群 G 及循环群 G 的生成元。

协议消息及所需的其他信息描述如下：

临时公钥 $R_B=g^b$，在 Z_q 中对应临时私钥 b；

临时公钥 $R_A=g^a$，在 Z_q 中对应临时私钥 a。

权标形式如下：

$Token_{AB}=R_A \| [Text_4] \| gsS_{AG}(R_A \| R_B \| [Text_3]) \| MAC_{AB}$；

$Token_{BA}=R_B \| [Text_6] \| gsS_{BG'}(R_B \| R_A \| [Text_5]) \| MAC_{BA}$。

其中：

$MAC_{AB}=mac_{MK}([Cert_G] \| R_A \| [Text_4] \| gsS_{AG}(R_A \| R_B \| [Text_3]))$；

$MAC_{BA}=mac_{MK}([Cert_{G'}] \| R_B \| [Text_6] \| gsS_{BG}(R_B \| R_A \| [Text_5]))$。

本机制执行过程如下：

a） A 执行下列步骤：

1） 从 Z_q 中选择临时私钥 a，计算临时公钥 $R_A=g^a$；

2） 发送 R_A、可选证书字段 $Cert_G$ 和可选文本字段 $Text_1$ 到 B。

a′） B 执行下列步骤：

1） 从 Z_q 中选择临时私钥 b，计算临时公钥 $R_B=g^b$；

2） 发送 R_B、可选证书字段 $Cert_{G'}$ 和可选文本字段 $Text_2$ 到 B。

b） A 和 B 通过验证群组公钥证书或其他方式获得对端实体所在群组的有效群组公钥。

c） A 执行下列步骤：

1） 计算 $g^{ab}=(R_B)^a$；

2） 计算 MAC 密钥 $MK=kgf(g^{ab})$；

3） 用签名密钥计算 $gsS_{AG}=(R_A \| R_B \| Text_3)$；

4） 用 MAC 密钥 MK 计算：

$MAC_{AB}=mac_{MK}([Cert_G] \| R_A \| [Text_4] \| gsS_{AG}(R_A \| R_B \| [Text_3]))$；

5） 发送 MAC_{AB} 到 B。

c′） B 执行下列步骤：

1） 计算 $g^{ab}=(R_A)^b$；

2） 计算 MAC 密钥 $MK=kgf(g^{ab})$；

3） 用签名密钥计算 $gsS_{BG'}=(R_B \| R_A \| Text_5)$；

4） 用 MAC 密钥 MK 计算：

$MAC_{BA}=mac_{MK}([Cert_{G'}]\|R_B\|[Text_6]\|gsS_{BG'}(R_B\|R_A\|[Text_5]))$；

5） 发送 $Token_{BA}$ 到 A。

d） A 和 B 执行下列步骤：

通过下列方式校验 $Token_{AB}$ 和 $Token_{BA}$：

1） 各自验证包含在权标中的群组签名；

2） 检查包含在群组签名中的临时公钥 R_A 和 R_B；

3） A 检查包含在 $Token_{BA}$ 中的临时公钥 R_B 与在步骤 a′）中收到的临时公钥 R_B 是否一致，检查包含在权标 $Token_{BA}$ 中的群组签名中的 R_A 与在步骤 a）中发送的临时公钥 R_A 是否一致；

4） B 检查包含在 $Token_{AB}$ 中的临时公钥 R_A 与在步骤 a）中收到的临时公钥 R_A 是否一致，检查包含在权标 $Token_{AB}$ 中的群组签名中的 R_B 与在步骤 a′）中发送的临时公钥 R_B 是否一致；

5） 各自用 MK 验证 MAC_{AB} 和 MAC_{BA} 的值。

7.5.5 机制 12——两次传递并行的签名在先双向鉴别

该带有绑定特性的两次传递并行的签名在先的双向鉴别协议中，实体发送的第一条消息包含群组签名，匿名鉴别过程在群组 G 中的实体 A 和群组 G' 中的实体 B 间执行。惟一性或时效性通过产生并检查随机数（参见 ISO/IEC 9798-1:2010[3]的附录 B）来控制。协议如图 11 所示。

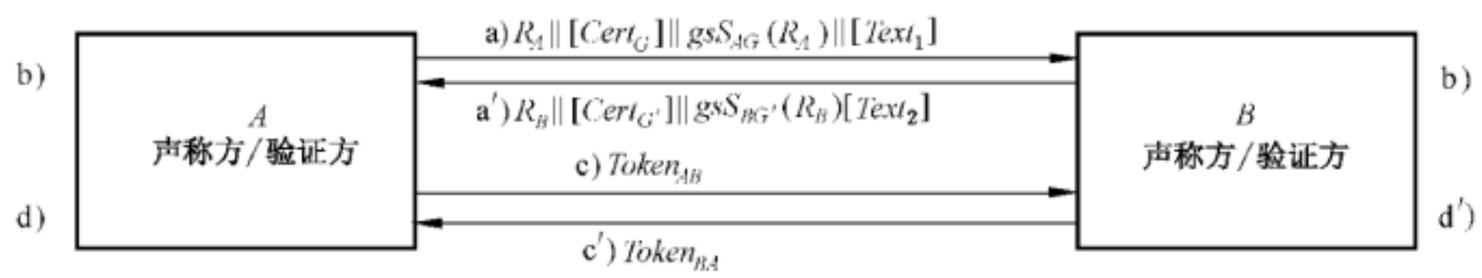

图 11 两次传递并行的签名在先双向匿名鉴别

在执行本机制时，应满足下列要求：

——考虑到 DDH 难解问题，实体 A 和实体 B 一定要协商 q 阶的循环群 G 及循环群 G 的生成元。

协议消息及所需的其他信息描述如下：

临时公钥 $R_B=g^b$，在 Z_q 中对应临时私钥 b；

临时公钥 $R_A=g^a$，在 Z_q 中对应临时私钥 a。

权标形式如下：

$Token_{AB}=MAC_{AB}\|[Text_3]$；

$Token_{BA}=MAC_{BA}\|[Text_4]$。

其中：

$MAC_{AB}=mac_{MK}(R_A\|gsS_{AG}(R_A)\|R_B\|gsS_{BG'}(R_B)\|[Text_5])$；

$MAC_{BA}=mac_{MK}(R_B\|gsS_{BG'}(R_B)\|R_A\|gsS_{AG}(R_A)\|[Text_6])$。

本机制执行过程如下：

a） A 执行下列步骤：

1） 从 Z_q 中选择临时私钥 a，计算临时公钥 $R_A=g^a$；

2） 用签名密钥计算 $gsS_{AG}(R_A)$；

3） 发送 g^a、$gsS_{AG}(R_A)$、可选证书字段 $Cert_G$ 和可选文本字段 $Text_1$ 到 B。

a′） B 执行下列步骤：

1） 从 Z_q 中选择临时私钥 b，计算临时公钥 $R_B=g^b$；

2） 用签名密钥计算 $gsS_{BG'}(R_B)$；

3） 发送 g^b、$gsS_{BG'}(R_B)$、可选证书字段 $Cert_{G'}$ 和可选文本字段 $Text_2$ 到 B。

b） A 和 B 通过验证群组公钥证书或其他方式获得对端实体所在群组的有效群组公钥，并验证收到的群组签名。

c） A 执行下列步骤：

1） 计算 $g^{ab}=(R_B)^a$；

2） 计算 MAC 密钥 $MK=kgf(g^{ab})$；

3） 用 MAC 密钥 MK 计算：

$MAC_{AB}=mac_{MK}(R_A \| gsS_{AG}(R_A) \| R_B \| gsS_{BG'}(R_B) \| [Text_5])$；

4） 发送 $Token_{AB}$ 到 B。

c′） B 执行下列步骤：

1） 计算 $g^{ab}=(R_A)^b$；

2） 计算 MAC 密钥 $MK=kgf(g^{ab})$；

3） 用 MAC 密钥 MK 计算：

$MAC_{BA}=mac_{MK}([Cert_G \| R_A \| [Text_3] \| gsS_{AG}(R_A \| R_B \| [Text_2])])$；

4） 发送 $Token_{BA}$ 到 A。

d） A 执行下列步骤：

1） 在步骤 a′）中获得临时公钥 R_B 和 $gsS_{BG'}(R_B)$；

2） 使用 MAC 密钥 MK 计算：

$MAC_{BA}=mac_{MK}([R_B \| gsS_{BG}(R_B) \| R_A \| gsS_{AG}(R_A) \| [Text_6]])$；

3） 用步骤 2）中计算得出的值检查在步骤 c′）中收到的权标中的 MAC_{BA} 的有效性。

d′） B 执行下列步骤：

1） 在步骤 a）中获得临时公钥 R_A 和 $gsS_{AG}(R_A)$；

2） 用 MAC 密钥 MK 计算：

$MAC_{AB}=mac_{MK}(R_A \| gsS_{AG}(R_A) \| R_B \| gsS_{BG'}(R_B) \| [Text_5])$；

3） 用步骤 2）中计算得出的值检查在步骤 c）中收到的权标中的 MAC_{AB} 的有效性。

7.6 带有绑定特性的单向匿名双向鉴别

7.6.1 总则

带有绑定特性的单向匿名双向鉴别是指两个实体双向鉴别，但是对于鉴别方来说，被鉴别方的真实身份是不被透漏的，绑定特性用于提供这种保证。

7.6 规定了带有绑定特性的单向匿名双向鉴别协议的细节。群组 G 中的实体 A 被实体 B 采用 ISO/IEC 20008-2 中规范的群组数字签名机制进行匿名鉴别，而实体 B 被群组 G 中的实体 A 采用 ISO/IEC 14888-3 或 ISO/IEC 9796 中规范的数字签名机制进行鉴别。

注：视情况，在 7.6 的机制中，实体 A 和 B 可从共享秘密中导出会话秘钥，用于它们之间后续的保密通信。但这在本部分的范围之外。

7.6.2 机制 13——三次传递签名在后单向匿名双向鉴别

改带有绑定特性的三次传递单向匿名双向鉴别协议中，实体发送的第一条消息不包含群组签名，由群组 G 中的实体 A 向实体 B 发起鉴别。惟一性或时效性通过产生并检查随机数（参见 ISO/IEC 9798-1:2010[3]的附录 B）来控制。协议如图 8 所示。

——考虑到 DDH 难解问题，实体 A 和实体 B 一定要协商 q 阶的循环群 G 及循环群 G 的生成元。

协议消息及所需的其他信息描述如下：

临时公钥 $R_B=g^b$，在 Z_q 中对应临时私钥 b；

临时公钥 $R_A=g^a$，在 Z_q 中对应临时私钥 a。

权标形式如下：

$Token_{BA}=R_B \| [Text_3] \| sB_B(R_B \| R_A \| [Text_2]) \| MAC_{BA}$；

$Token_{AB}=R_A \| [Text_5] \| gsS_{AG}(R_A \| R_B \| [Text_4]) \| MAC_{AB}$。

其中：

$MAC_{AB}=mac_{MK}([Cert_B] \| R_B \| [Text_3] \| sS_B(R_B \| R_A \| [Text_2]))$；

$MAC_{AB}=mac_{MK}([Cert_G] \| R_B \| [Text_5] \| gsS_{AG}(R_A \| R_B \| [Text_4]))$。

本机制执行过程如下：

a) A 执行下列步骤：

1) 从 Z_q 中选择临时私钥 a，计算临时公钥 $R_A=g^a$；

2) 发送 g^a、可选文本字段 $Text_1$ 到 B。

b) B 执行下列步骤：

1) 从 Z_q 中选择临时私钥 b，计算临时公钥 $R_B=g^b$；

2) 计算 $g^{ab}=(R_A)^b$；

3) 计算 MAC 密钥 $MK=kgf(g^{ab})$；

4) 用签名密钥计算 $sS_B(R_B \| R_A \| [Text_2])$；

5) 用 MAC 密钥 MK 计算：

$MAC_{BA}=mac_{MK}([Cert_B] \| R_B \| [Text_3] \| sS_B(R_B \| R_A \| [Text_2]))$；

6) 发送 $Token_{BA}$、可选证书字段 $Cert_B$ 到 A。

c) 收到权标 $Token_{BA}$，A 执行下列步骤：

1) 计算 $g^{ab}=(R_B)^a$。

2) 计算 MAC 密钥 $MK=kgf(g^{ab})$。

3) 通过验证 B 的公钥证书或其他方式获得 B 的有效公钥。

4) 通过下列方式校验 $Token_{BA}$：

i) 验证包含在 $Token_{BA}$ 中 B 的签名；

ii) 检查包含在签名中的临时公钥 R_B 和 R_A；

iii) 检查包含在 $Token_{BA}$ 中的临时公钥 R_A 与在步骤 a)中发送的临时公钥 R_A 是否一致；

iv) 使用 MK 来检查 MAC_{BA} 的值。

5) 用签名密钥计算 $gsS_{AG}(R_A \| R_B \| Text_4)$。

6) 用 MAC 密钥 MK 计算：

$MAC_{AB}=mac_{MK}([Cert_G] \| R_B \| [Text_3] \| gsS_{AG}(R_A \| R_B \| [Text_4]))$。

d) A 发送 $Token_{AB}$ 和可选证书字段 $Cert_G$ 到 B。

e) 收到包含在 $Token_{AB}$ 的消息后，B 执行下列步骤：

1) 通过验证 G 的群组公钥证书或其他方式获得 G 的有效群组公钥。

2) 通过下列方式校验 $Token_{AB}$：

i) 验证包含 $Token_{AB}$ 中的 A 的群组签名；

ii) 检查包含在群组签名中的临时公钥 R_A 和 R_B；

iii) 检查包含在 $Token_{AB}$ 中的临时公钥 R_A 与在步骤 a)收到的临时公钥 R_A 是否一致；

iv) 检查包含在 $Token_{AB}$ 的群组签名中的临时公钥 R_B 与在步骤 b)中发送的临时公钥 R_B 是否一致。

v) 用 MK 验证 MAC_{AB} 的值。

7.6.3 机制 14——三次传递签名在先单向匿名双向鉴别

该带有绑定特性的三次传递签名在先的单向匿名双向鉴别协议中，实体发送的第一条消息包含群组签名，由群组 G 中的实体 A 向实体 B 发起鉴别。惟一性或时效性通过产生并检查随机数(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。协议如图 12 所示。

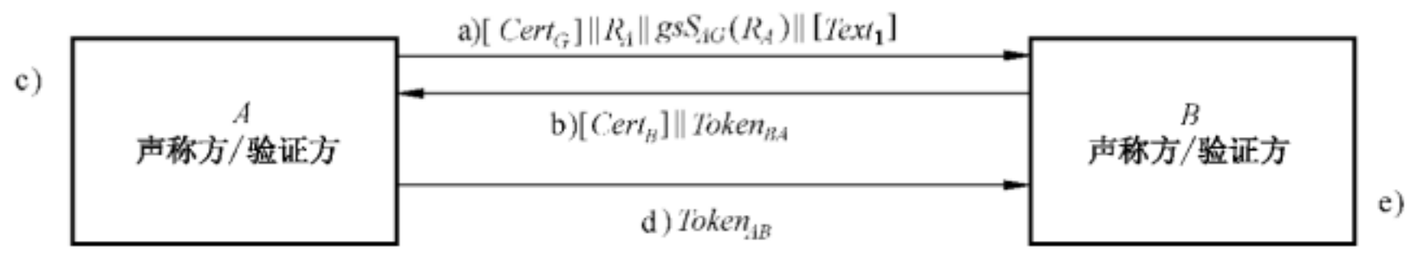

图 12 三次传递签名在先单向匿名双向鉴别

在执行本机制时，应满足下列要求。

——考虑到 DDH 难解问题，实体 A 和实体 B 一定要协商 q 阶的循环群 G 及循环群 G 的生成元。

协议消息及所需的其他信息描述如下：

临时公钥 $R_B=g^b$，在 Z_q 中对应临时私钥 b；

临时公钥 $R_A=g^a$，在 Z_q 中对应临时私钥 a。

权标形式如下：

$Token_{AB}=MAC_{AB}\parallel[Text_2]$；

$Token_{BA}=R_B\parallel sS_B(R_B)\parallel MAC_{BA}\parallel[Text_3]$。

其中：

$MAC_{AB}=mac_{MK}(R_A\parallel gsS_{AG}(R_A)\parallel R_B\parallel sS_B(R_B)\parallel[Text_4])$；

$MAC_{BA}=mac_{MK}(R_B\parallel sS_B(R_B)\parallel R_A\parallel gsS_{AG}(R_A)\parallel[Text_5])$。

本机制执行过程如下：

a) A 执行下列步骤：

1) 从 Z_q 中选择临时私钥 a，计算临时公钥 $R_A=g^a$；

2) 用签名密钥计算 $gsS_{AG}(R_A)$；

3) 发送 g^a、$gsS_{AG}(R_A)$、可选证书字段 $Cert_G$ 和可选文本字段 $Text_1$ 到 B。

b) B 执行下列步骤：

1) 通过验证 G 的群组公钥证书或其他方式获得 G 的有效群组公钥；

2) 验证 A 的群组签名；

3) 从 Z_q 中选择临时私钥 b，计算临时公钥 $R_B=g^b$；

4) 用签名密钥计算 $gsS_B(R_B)$；

5) 计算 $g^{ab}=(R_A)^b$；

6) 计算 MAC 密钥 $MK=kgf(g^{ab})$；

7) 使用 MAC 密钥 MK 计算：

$MAC_{BA}=mac_{MK}(R_B\parallel sS_B(R_B)\parallel R_A\parallel gsS_{AG}(R_A)\parallel[Text_5])$；

8) 发送 $Token_{BA}$ 和可选证书字段 $Cert_B$ 到 A。

c) 收到包含权标 $Token_{BA}$ 的消息后，A 执行下列步骤：

1) 通过验证 B 的公钥证书或其他方式获得 B 的有效公钥；

2) 验证 B 的签名；

3) 计算 $g^{ab}=(R_B)^a$；

4) 计算 MAC 密钥 $MK=kgf(g^{ab})$；

5) 用 MAC 密钥 MK 计算：

$MAC_{AB}=mac_{MK}(R_A \| gsS_{AG}(R_A) \| R_B \| sS_B(R_B) \| [Text_4])$；

6) 用 MK 验证 MAC_{BA} 的值。

d) A 发送 $Token_{AB}$ 到 B。

e) 收到包含 $Token_{AB}$ 的消息，B 用 MK 验证 MAC_{AB} 的值。

7.6.4 机制 15——两次传递并行的签名在后单向匿名双向鉴别

该带有绑定特性的两次传递并行的签名在后的单向匿名双向鉴别协议中，实体发送的第一条消息不包含群组签名，匿名鉴别过程在群组 G 中的实体 A 和实体 B 之间并行的执行。惟一性或时效性通过产生并检查随机数(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。协议如图 9 所示。

在执行本机制时，应满足下列要求：

——考虑到 DDH 难解问题，实体 A 和实体 B 一定要协商 q 阶的循环群 G 及循环群 G 的生成元。

协议消息及所需的其他信息描述如下：

临时公钥 $R_B=g^b$，在 Z_q 中对应临时私钥 b；

临时公钥 $R_A=g^a$，在 Z_q 中对应临时私钥 a。

权标形式如下：

$Token_{AB}=R_A \| [Text_4] \| gsS_{AG}(R_A | R_B \| [Text_3]) \| MAC_{AB}$；

$Token_{BA}=R_B \| [Text_6] \| sS_B(R_B \| R_A \| [Text_5]) \| MAC_{BA}$。

其中：

$MAC_{AB}=mac_{MK}([Cert_G] \| R_A \| [Text_4] \| gsS_{AG}(R_A \| R_B \| [Text_3]))$；

$MAC_{BA}=mac_{MK}([Cert_B] \| R_B \| [Text_6] \| sS_B(R_B \| R_A \| [Text_5]))$。

本机制执行过程如下：

a) A 执行下列步骤：

1) 从 Z_q 中选择临时私钥 a，计算临时公钥 $R_A=g^a$；

2) 发送 R_A、群组公钥证书 $Cert_G$(可选)和文本值 $Text_1$ 给 B。

a′) B 执行下列步骤：

1) 从 Z_q 中选择临时私钥 b，计算临时公钥 $R_B=g^b$；

2) 发送 R_B、可选证书字段 $Cert_B$ 和可选文本字段 $Text_2$ 到 A。

b) A 和 B 各自通过验证对端的公钥证书或其他方式获得对端的有效公钥。

c) A 执行下列步骤：

1) 计算 $g^{ab}=(R_B)^a$；

2) 计算 MAC 密钥 $MK=kdf(g^{ab})$；

3) 用签名密钥计算 $gsS_{AG}(R_A \| R_B \| [Text_3])$；

4) 用 MAC 密钥 MK 计算：

$MAC_{AB}=mac_{MK}([Cert_G] \| R_A \| [Text_4] \| gsS_{AG}(R_A \| R_B \| [Text_3]))$；

5) 发送 $Token_{AB}$ 到 B。

c′) B 执行下列步骤：

1) 计算 $g^{ab}=(R_A)^b$；

2) 计算 MAC 密钥 $MK=kgf(g^{ab})$；

3) 用签名密钥计算 $sS_B(R_B \| R_A \| [Text_5])$；

4) 用 MAC 密钥 MK 计算：

$MAC_{BA}=mac_{MK}([Cert_B] \| R_B \| [Text_6] \| sS_B(R_B \| R_A \| [Text_5]))$；

5) 发送 $Token_{AB}$ 到 A。

d) A 和 B 执行下列步骤：

1) A 和 B 按照如下步骤校验 $Token_{AB}$ 和 $Token_{BA}$：

i) 验证包含在权标中的签名或群组签名；

ii) 检查包含在签名或群组签名中的临时公钥 R_A 和 R_B；

iii) A 检查包含在 $Token_{BA}$ 中的临时公钥 R_B 与在步骤 a′)中收到的临时公钥 R_B 是否一致，检查包含在 $Token_{BA}$ 的签名中的临时公钥 R_A 与在步骤 a)中发送的 R_A 是否一致；

iv) B 检查包含在 $Token_{AB}$ 中的临时公钥 R_A 与在步骤 a)中收到的临时公钥 R_A 是否一致，检查包含在 $Token_{AB}$ 的签名中的临时公钥 R_B 与在步骤 a′)中发送的 R_B 是否一致；

v) 用 MK 分别验证 MAC_{AB} 和 MAC_{BA} 的值。

7.6.5 机制 16——两次传递并行的签名在先单向匿名双向鉴别

该带有绑定特性的两次传递并行的签名在先的单向匿名双向鉴别协议中，实体发送的第一条消息包含群组签名，匿名鉴别过程在群组 G 中的实体 A 和实体 B 之间并行的执行。惟一性或时效性通过产生并检查随机数(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。协议如图 13 所示。

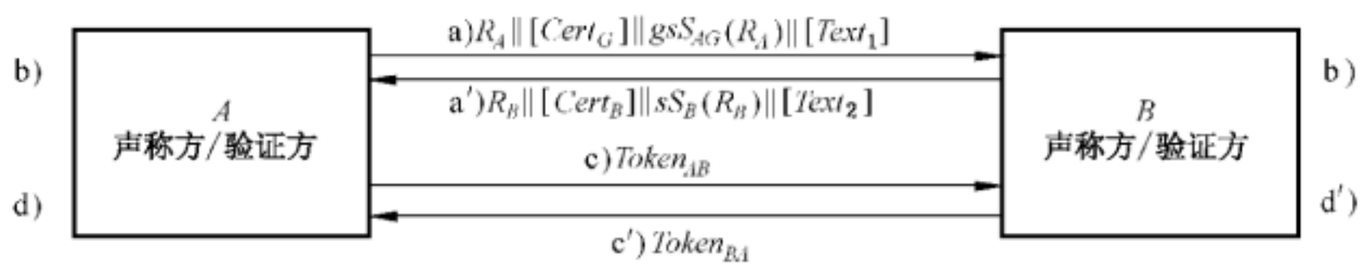

图 13 两次传递并行的签名在先单向匿名双向鉴别

在执行本机制时，应满足下列要求

——考虑到 DDH 难解问题，实体 A 和实体 B 一定要协商 q 阶的循环群 G 及循环群 G 的生成元。

协议消息及所需的其他信息描述如下：

临时公钥 $R_B = g^b$，在 Z_q 中对应临时私钥 b；

临时公钥 $R_A = g^a$，在 Z_q 中对应临时私钥 a。

权标形式如下：

$Token_{AB} = MAC_{AB} \| [Text_3]$；

$Token_{BA} = MAC_{BA} \| [Text_4]$。

其中：

$MAC_{AB} = mac_{MK}(R_A \| gsS_{AG}(R_A) \| R_B \| sS_B(R_B) \| [Text_5])$；

$MAC_{BA} = mac_{MK}(R_B \| sS_B(R_B) \| R_A \| gsS_{AG}(R_A) \| [Text_6])$。

本机制执行过程如下：

a) A 执行下列步骤：

1) 从 Z_q 中选择临时私钥 a，计算临时公钥 $R_A = g^a$；

2) 用签名密钥计算 $gsS_{AG}(R_A)$；

3) 发送 g^a、$gsS_{AG}(R_A)$、可选证书字段 $Cert_G$ 和可选文本字段 $Text_1$ 到 B。

a′) B 执行下列步骤：

1) 从 Z_q 中选择临时私钥 b，计算临时公钥 $R_B = g^b$；

2) 用签名密钥计算 $gsS_{BG'}(R_B)$；

3) 发送 g^b、$gsS_{BG'}(R_B)$、可选证书字段 $Cert_{G'}$ 和可选文本字段 $Text_2$ 到 B。

b) A 和 B 各自通过验证对端的公钥证书或其他方式获得对端的有效公钥，并各自验证收到的签名和群组签名。

c) A 执行下列步骤：

1) 计算 $g^{ab}=(R_B)^a$；

2) 计算 MAC 密钥 $MK=kgf(g^{ab})$；

3) 用 MAC 密钥 MK 计算：

$MAC_{AB}=mac_{MK}(R_A \| gsS_{AG}(R_A) \| R_B \| sS_B(R_B) \| [Text_5])$；

4) 发送 $Token_{AB}$ 到 B。

c′) B 执行下列步骤：

1) 计算 $g^{ab}=(R_B)^a$；

2) 计算 MAC 密钥 $MK=kgf(g^{ab})$；

3) 使用 MAC 密钥 MK 计算：

$MAC_{BA}=mac_{MK}(R_B \| sS_B(R_B) \| R_A \| gsS_{AG}(R_A) \| [Text_6])$；

4) 发送 $Token_{BA}$ 到 A。

d) A 执行下列步骤：

1) 在步骤 a′)中获得临时公钥 R_B 和签名 $sS_B(R_B)$；

2) 用 MAC 密钥 MK 计算：

$MAC_{BA}=mac_{MK}(R_B \| sS_B(R_B) \| R_A \| gsS_{AG}(R_A) \| [Text_6])$；

3) 用在子步骤 2)中计算得到的值验证在步骤 c′)中收到的权标中 MAC_{BA} 的有效性。

d′) B 执行下列步骤：

1) 在步骤 a)中获得临时公钥 R_A 和签名 $gsS_{AG}(R_A)$；

2) 用 MAC 密钥 MK 计算：

$MAC_{AB}=mac_{MK}(R_A \| gsS_{AG}(R_A) \| R_B \| sS_B(R_B) \| [Text_5])$；

3) 用在子步骤 2)中计算得到的值验证在步骤 c)中收到的权标中 MAC_{AB} 的有效性。

8 有在线可信第三方参与的匿名鉴别机制

8.1 概述

本章规定了有在线可信第三方参与的匿名实体鉴别机制。

本章的匿名鉴别机制需要 G 中的实体 A 和/或 G' 中的实体 B 两个实体利用在线可信第三方(TP)验证彼此的群组公钥。该可信第三方应持有 G(A 归属的群组)和 G'(B 归属的群组)的群组公钥的可靠副本，实体 A 和 B 应持有 TP 的公钥的可靠副本。

机制的实施应采用 ISO/IEC 20008-2 中规定的群组签名方案中的一种。

8.2 单向匿名鉴别

8.2.1 总则

单向匿名鉴别是指两个实体只有其中一个实体被鉴别，并且该实体对于另外一个实体是匿名的。

8.2.2 机制 17——四次传递单向匿名鉴别(由实体 A 发起)

在本机制中，实体 A 向属于群组 G' 的实体 B 发起鉴别协议。惟一性或时效性通过产生并检查随机数(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。协议如图 14 所示。

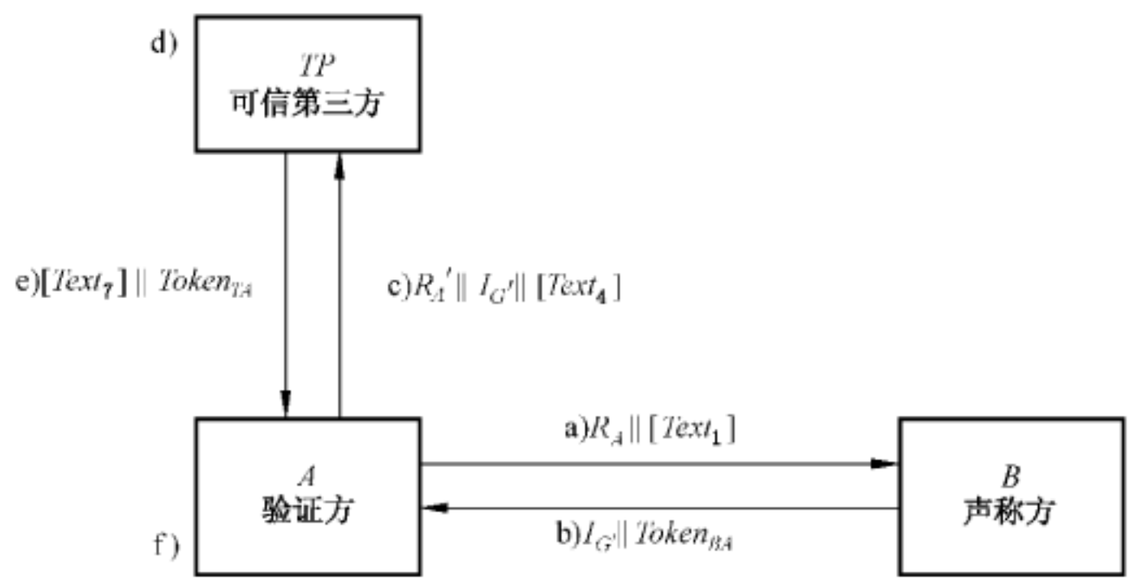

图 14　四次传递单向匿名鉴别(实体 A 发起)

权标形式如下：

$Token_{BA}=[Text_3] \parallel gsS_{BG'}(A \parallel R_A \parallel [Text_2])$；

$Token_{TA}=Res_{G'} \parallel sS_T(R_A' \parallel Res_{G'} \parallel [Text_6])$。

字段 $I_{G'}$、$Res_{G'}$、$Status$ 和 $Failure$ 的值如下所示：

G'：实体 B 所属的群组；

$I_{G'}$：群组 G'的身份，为 G'或 $Cert_{G'}$；

$Res_{G'}=(Cert_{G'} \parallel Status)$，$(G' \parallel P_{G'})$或 $Failure$；

$Status=True$ 或 $False$。如果证书已经被撤消，则这个字段的值应为 $False$，否则这个字段应为 $True$；

$Failure$：当 TP 无法获得 G'的公钥或者证书，则 $Res_{G'}$字段的值应为 $Failure$。

在本机制中，如果 TP 确认 G'身份和 $P_{G'}$之间的映射关系，则 $I_{G'}=G'$；否则，$I_{G'}=Cert_{G'}$，并且 G'应设置等于 $Cert_{G'}$的可区分标识符字段值。如果 G'或者 $Cert_{G'}$允许被用于作为一种身份，则宜允许 TP 区分这两种类型的身份标识。$Res_{G'}$的值应按表 1 确定。

表 1　$Res_{G'}$ 的值

域	选项 1	选项 2
$I_{G'}$	G'	$Cert_{G'}$
$Res_{G'}$	$(G' \parallel P_{G'})$或 $Failure$	$(Cert_{G'} \parallel Status)$或 $Failure$

本机制的执行过程如下：

a)　A 发送随机数 R_A 和可选文本字段 $Text_1$到 B。

b)　B 发送 $Token_{BA}$和身份 $I_{G'}$到 A。

c)　A 发送随机数 R_A'、身份 $I_{G'}$和可选文本字段 $Text_4$到 TP。

d)　收到来自步骤 c)中 A 的消息后，TP 执行下列步骤：如果 $I_{G'}=G'$，则 TP 提取 $P_{G'}$；如果 $I_{G'}=Cert_{G'}$，则 TP 检查 $Cert_{G'}$的有效性。

e)　TP 发送 $Token_{TA}$和可选文本字段 $Text_7$ 到 A。$Token_{TA}$中的 $Res_{G'}$字段应为 G'的证书及其状态，或者是 G'的可区分标识符及其公钥，或者是指示符 $Failure$。

f)　收到来自步骤 e)中 TP 的消息后，A 执行下列步骤：

　1)　通过下列方式校验 $Token_{TA}$：验证包含在 $Token_{TA}$中的 TP 签名，检查在步骤 c)中发送给 TP 的随机数 R_A'与包含在 $Token_{TA}$中的 TP 的签名数据中的随机数 R_A'是否一致。

　2)　通过检查 $Res_{G'}$验证 G'的有效性。

　3)　从消息中提取 G'的公钥，通过下列方式校验 $Token_{BA}$：验证包含在 $Token_{BA}$中的 B 的匿

名签名，检查 $Token_{BA}$ 中的被签名消息中的标识符域的值(A)与 A 的可区分标识符是否一致，检查包含在 $Token_{BA}$ 中的随机数 R_A 与在步骤 a)中发送给 B 的随机数 R_A 是否一致。

8.2.3 机制 18——四次传递单向匿名鉴别(由实体 *B* 发起)

在本机制中，实体 B 向属于群组 G 的实体 A 发起鉴别协议。惟一性或时效性通过产生并检查随机数(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。协议如图 15 所示。

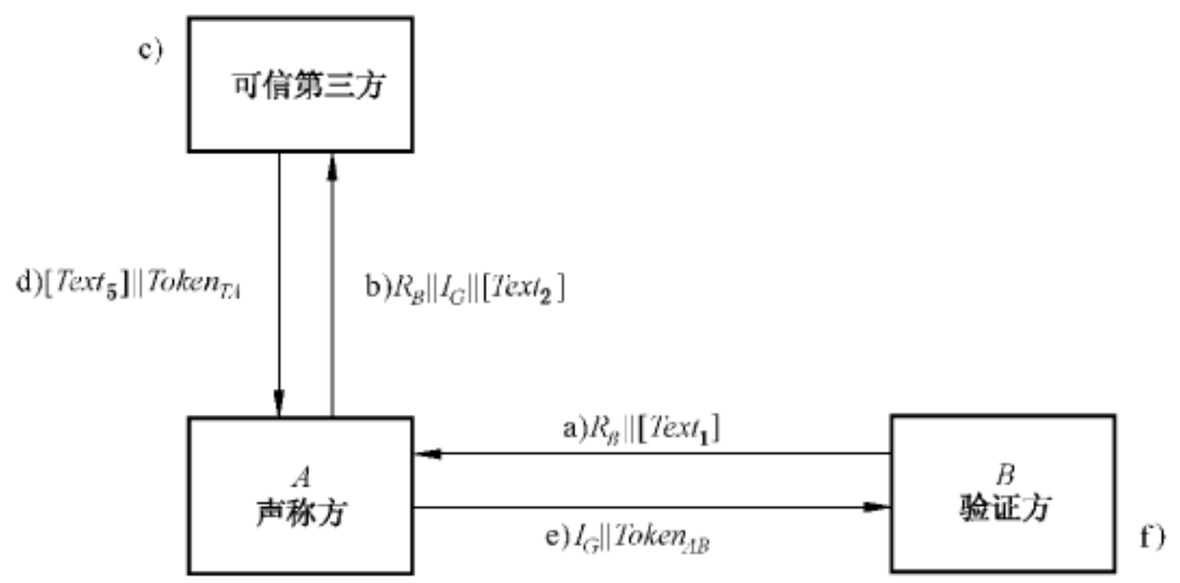

图 15 四次传递单向匿名鉴别(由实体 *B* 发起)

权标形式如下：

$Token_{AB}=Res_G \parallel sS_T(R_B \parallel Res_G \parallel [Text_3]) \parallel gsS_{AG}(R_B \parallel B \parallel [Text_6])$；

$Token_{TA}=Res_G \parallel sS_T(R_B \parallel Res_G \parallel [Text_3])$。

字段 I_G、Res_G、$Status$ 和 $Failure$ 的值如下所示：

G：实体 A 所属的群组；

I_G：群组 G 的身份，为 G 或 $Cert_G$；

$Res_G=(Cert_G \parallel Status),(G \parallel P_G)$或 $Failure$；

$Status=True$ 或 $False$。如果证书已经被撤消，则这个字段的值应为 $False$，否则这个字段应为 $True$；

$Failure$：当 TP 无法获得 G 的公钥或者证书，则 Res_G 字段的值应为 $Failure$。

在本机制中，如果 TP 确认 G 身份和 P_G 之间的映射关系，则 $I_G=G$；否则，$I_G=Cert_G$，并且 G 应设置等于 $Cert_G$ 的可区分标识符字段值。如果 G 或者 $Cert_G$ 允许被用于作为一种身份，则宜允许 TP 区分这两种类型的身份标识。Res_G 的值应按表 2 确定。

表 2 Res_G 的值

字段	选项 1	选项 2
I_G	G	$Cert_G$
Res_G	$(G \parallel P_G)$或 $Failure$	$(Cert_G \parallel Status)$或 $Failure$

本机制的执行过程如下：

a) B 发送随机数 R_B 和可选文本字段 $Text_1$ 到 A。

b) A 发送随机数 R_B、身份 I_G 和可选文本字段 $Text_2$ 到 TP。

c) 收到来自步骤 b)中 A 的消息后，TP 执行下列步骤：如果 $I_G=G$，则 TP 提取 P_G；如果 $I_G=Cert_G$，则 TP 检查 $Cert_G$ 的有效性。

d) TP 发送 $Token_{TA}$ 和可选文本字段 $Text_5$ 到 A。$Token_{TA}$ 中的 Res_G 字段应为 G 的证书及其状

态，或者是 G 的可区分标识符及其公钥，或者是指示符 $Failure$；

e) A 发送权标 $Token_{AB}$ 和身份 I_G 到 B。

f) 收到来自步骤 e)中 A 的消息后，B 执行下列步骤：

1) 通过下列方式验证 $Token_{AB}$ 中 TP 的签名：检查在步骤 a)中发送给 A 的随机数 R_B 与包含在 $Token_{AB}$ 中的 TP 签名数据中的随机数 R_B 是否一致。

2) 通过检查 Res_G 验证 G 的有效性。

3) 从消息中提取 G 的公钥，通过下列方式校验 $Token_{AB}$：验证包含在 $Token_{AB}$ 中的 A 的匿名签名，检查 $Token_{AB}$ 中的被签名消息中的标识符域的值(B)与 B 的可区分标识符是否一致，检查包含在 $Token_{AB}$ 中的 A 的签名数据中的随机数 R_B 与在步骤 a)中发送给 A 的随机数 R_B 是否一致。

8.3 双向匿名鉴别

8.3.1 总则

双向匿名鉴别是指两个实体双向鉴别，并且两个实体的身份在鉴别时对对方是匿名的。

8.3.2 机制 19——五次传递双向匿名鉴别(由实体 A 发起)

在本机制中，属于群组 G 的实体 A 向属于群组 G' 的实体 B 发起鉴别协议。惟一性或时效性通过产生并检查随机数(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。协议如图 16 所示。

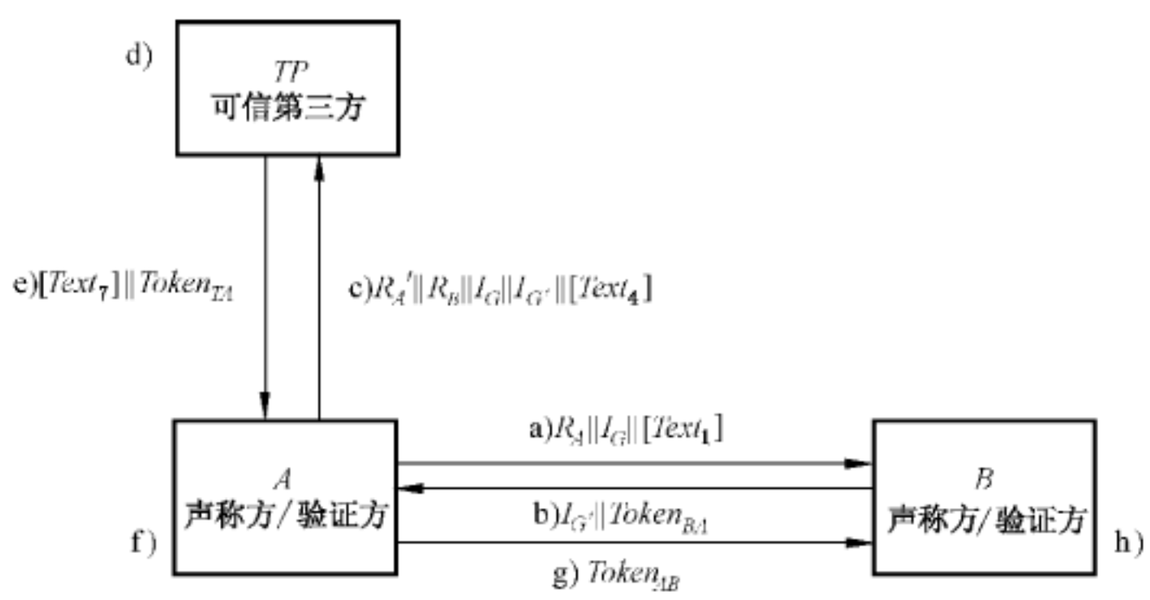

图 16 五次传递双向匿名鉴别(由实体 A 发起)

权标应为如下两种形式。

选项 1：

$Token_{BA}=R_A \parallel R_B \parallel [Text_3] \parallel gsS_{BG'}(G' \parallel R_A \parallel R_B \parallel G \parallel [Text_2])$；

$Token_{TA}=Res_G \parallel Res_{G'} \parallel sS_T(R_A' \parallel Res_{G'} \parallel [Text_6]) \parallel sS_T(R_B \parallel Res_G \parallel [Text_5])$；

$Token_{AB}=[Text_9] \parallel [Res_G] \parallel sS_T(R_B \parallel Res_G \parallel [Text_5] \parallel gsS_{AG}(R_B \parallel R_A \parallel G' \parallel G \parallel [Text_8])$。

选项 2：

$Token_{BA}=R_A \parallel R_B \parallel [Text_3] \parallel gsS_{BG'}(G' \parallel R_A \parallel R_B \parallel G \parallel [Text_2])$；

$Token_{TA}=Res_G \parallel Res_{G'} \parallel sS_T(R_A' \parallel R_B \parallel Res_G \parallel Res_{G'} \parallel [Text_5])$；

$Token_{AB}=R_A' \parallel [Text_9] \parallel Token_{TA} \parallel gsS_{AG}(R_B \parallel R_A \parallel G' \parallel G \parallel [Text_8])$。

字段 I_G，$I_{G'}$，Res_G，$Res_{G'}$ 的值以及 $Status$ 和 $Failure$ 如下所示：

I_G：群组 G 的身份，可以为 G 或者 $Cert_G$；

$I_{G'}$：群组 G' 的身份，可以为 G' 或者 $Cert_{G'}$；

$Res_G=(Cert_G \parallel Status)$，$(G \parallel P_G)$或 $Failure$；

$Res_{G'}=(Cert_{G'} \parallel Status)$，$(G' \parallel P_G{}')$或 $Failure$；

$Status=True$ 或 $False$ 。如果证书已经被撤消，则这个字段的值应为 $False$，否则这个字段应为 $True$；

$Failure$：当 TP 无法获得 G 的公钥或者证书，则 Res_G 字段的值应为 $Failure$。

在本机制中，如果 TP 确认 G 身份和 P_G之间的映射关系，则 $I_G=G$；否则，$I_G=Cert_G$，并且 G 应设置等于 $Cert_G$的可区分标识符字段值。如果 G 或者 $Cert_G$允许被用于作为一种身份，则宜允许 TP 区分这两种类型的身份标识。Res_G 的值应按表 3 确定。

表 3　Res_G 的值

字段	选项 1	选项 2
I_G	G	$Cert_G$
Res_G	$(G \parallel P_G)$或 $Failure$	$(Cert_G \parallel Status)$或 $Failure$

本机制的执行过程如下：

a)　A 发送随机数 R_A，身份 I_G 和可选文本字段 $Text_1$到 B。

b)　B 发送 $Token_{BA}$和身份 $I_{G'}$到 A。

c)　A 发送随机数 $R_A{}'$、R_B，身份 I_G、$I_{G'}$和可选文本字段 $Text_4$到 TP。

d)　收到来自步骤 c)中 A 的消息后，执行下列步骤：如果 $I_G=G$，且 $I_{G'}=G'$，则 TP 提取 P_G 和 $P_{G'}$；如果 $I_G=Cert_G$，且 $I_{G'}=Cert_{G'}$，则 TP 检查 $Cert_G$ 和 $Cert_{G'}$的有效性。

e)　TP 发送 $Token_{TA}$和可选文本字段 $Text_7$ 到 A。$Token_{TA}$中的 Res_G 和 $Res_{G'}$字段应为 G 和 G'的证书及它们的状态，或者是 G 和 G'的可区分标识符及它们的公钥，或者是指示符 $Failure$。

f)　收到来自步骤 e)中 TP 的消息后，A 执行下列步骤：

　1)　通过下列方式校验 $Token_{TA}$：验证包含在 $Token_{TA}$中 TP 的签名，检查在步骤 c)中发送给 TP 的随机数 $R_A{}'$与包含在 $Token_{TA}$中被签名消息中的随机数 $R_A{}'$是否一致。

　2)　从消息中提取 G'的公钥，通过下列方式校验 $Token_{BA}$：验证包含在 $Token_{BA}$中的 B 的匿名签名，检查 $Token_{BA}$中的被签名消息中的标识符域的值(A)与 A 的可区分标识符是否一致，检查包含在 $Token_{BA}$中的随机数 R_A 与在步骤 a)中发送给 B 的随机数 R_A 是否一致。

g)　A 发送 $Token_{AB}$到 B。

h)　收到来自步骤 g)中 A 的消息后，B 执行下列步骤：

　1)　通过下列方式校验 $Token_{TA}$：验证包含在 $Token_{TA}$中 TP 的签名，检查在步骤 b)中发送给 A 的随机数 R_B与包含在 $Token_{AB}$中被签名消息中的随机数 R_B是否一致。

　2)　从消息中提取 G 的公钥，通过下列方式校验 $Token_{AB}$：验证包含在 $Token_{AB}$中的 G 的群组签名，检查权标 $Token_{AB}$中被签名消息中的标识符域的值(G')与群组 G'的可区分标识符是否一致，检查包含在 $Token_{AB}$中被签名消息中的随机数 R_B 与在步骤 b)中发送给 A 的随机数 R_B 是否一致。

8.3.3　机制 20——五次传递双向匿名鉴别(由实体 *B* 发起)

在本机制中，属于群组 G'的实体 B 向属于群组 G 的实体 A 发起鉴别协议。惟一性或时效性通过产生并校验随机数(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。该鉴别机制如图 17 所示。

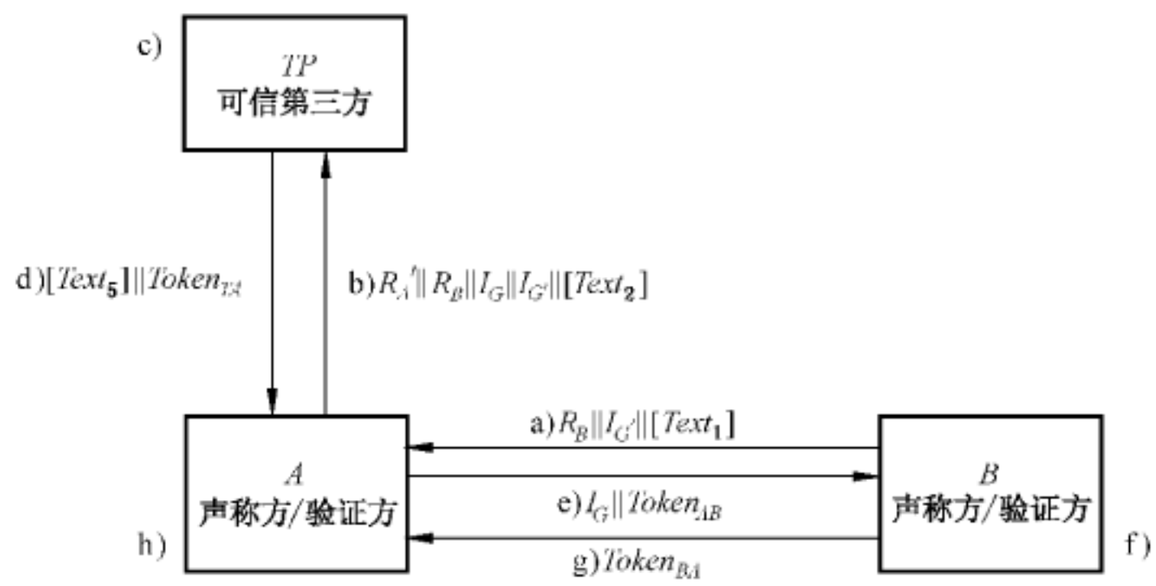

图 17　五次传递双向匿名鉴别(由实体 *B* 发起)

权标应为如下两种形式。

选项 1:

$Token_{BA}=R_A \parallel R_B \parallel [Text_9] \parallel gsS_{BG'}(G \parallel R_A \parallel R_B \parallel G' \parallel [Text_8])$;

$Token_{TA}=Res_G \parallel Res_{G'} \parallel sS_T(R_A' \parallel Res_{G'} \parallel [Text_4]) \parallel sS_T(R_B \parallel Res_G \parallel [Text_2])$;

$Token_{AB}=[Text_7] \parallel R_A \parallel Res_G \parallel sS_T(R_B \parallel Res_G \parallel [Text_3]) \parallel gsS_{AG}(R_B \parallel R_A \parallel G' \parallel G \parallel [Text_6])$。

选项 2:

$Token_{BA}=R_A \parallel R_B \parallel [Text_9] \parallel gsS_{BG'}(R_A \parallel R_B \parallel G \parallel G' \parallel [Text_8])$;

$Token_{TA}=Res_G \parallel Res_{G'} \parallel sS_T(R_A' \parallel R_B \parallel Res_G \parallel Res_{G'} \parallel [Text_3])$;

$Token_{AB}=R_A \parallel [Text_7] \parallel Token_{TA} \parallel gsS_{AG}(R_B \parallel R_A \parallel G' \parallel G \parallel [Text_6])$。

字段 I_G,$I_{G'}$,Res_G,$Res_{G'}$ 的值以及 *Status* 和 *Failure* 如下所示:

I_G:群组 G 的身份,为 G 或 $Cert_G$;

$I_{G'}$:群组 G' 的身份,为 G' 或 $Cert_{G'}$;

$Res_G=(Cert_G \parallel Status)$,$(G \parallel P_G)$或 *Failure*;

$Res_{G'}=(Cert_G \parallel Status)$,$(G' \parallel P_{G'})$或 *Failure*;

Status=*True* 或 *False*。如果证书已经被撤消,则这个字段的值应为 *False*,否则这个字段应为 *True*;

Failure:当 *TP* 无法获得 G 的公钥或者证书,则 Res_G 字段的值应为 *Failure*。

在本机制中,如果 *TP* 确认 G 身份和 P_G 之间的映射关系,则 $I_G=G$;否则,$I_G=Cert_G$,并且 G 应设置等于 $Cert_G$ 的可区分标识符字段值。如果 G 或者 $Cert_G$ 允许被用于作为一种身份,则宜允许 *TP* 区分这两种类型的身份标识。Res_G 的值应按表 4 确定。

表 4　Res_G 的值

字段	选项 1	选项 2
I_G	G	$Cert_G$
Res_G	$(G \parallel P_G)$或 *Failure*	$(Cert_G \parallel Status)$或 *Failure*

本机制的执行过程如下:

a)　*B* 发送随机数 R_B,身份 $I_{G'}$ 和可选文本字段 $Text_1$ 到 *A*。

b)　*A* 发送随机数 R_A'、R_B,身份 I_G、$I_{G'}$ 和可选文字字段 $Text_2$ 到 *TP*。

c)　收到来自步骤 b)中 *A* 的消息后,*TP* 执行以下步骤:如果 $I_G=G$,且 $I_{G'}=G'$,则 *TP* 提取 P_G 和 $P_{G'}$;如果 $I_G=Cert_G$,且 $I_{G'}=Cert_{G'}$,则 *TP* 检查 $Cert_G$ 和 $Cert_{G'}$ 的有效性。

d) TP 发送 $Token_{TA}$ 和可选文本字段 $Text_5$ 到 A。$Token_{TA}$ 中的 Res_G 和 $Res_{G'}$ 字段应为 G 和 G' 的证书及它们的状态，或者是 G 和 G' 的可区分标识符及它们的公钥，或者是指示符 $Failure$。

e) A 发送 $Token_{AB}$ 和身份 I_G 到 B。

f) 收到来自步骤 e)中 A 的消息后，B 执行下列步骤：

   1) 通过下列方式验证 $Token_{AB}$ 中 TP 的签名：检查在步骤 a)中发送给 A 的随机数 R_B 与包含在 $Token_{AB}$ 中的 TP 签名数据中的随机数 R_B 是否一致。

   2) 从消息中提取 G 的公钥，通过下列方式校验 $Token_{AB}$：验证包含在 $Token_{AB}$ 中的 A 的匿名签名，检查 $Token_{AB}$ 中的被签名消息中的标识符域的值(G')与群组 G' 的可区分标识符是否一致，检查包含在 $Token_{AB}$ 中的 A 的签名数据中的随机数 R_B 与在步骤 a)中发送给 A 的随机数 R_B 是否一致。

g) B 发送 $Token_{BA}$ 到 A。

h) 收到来自步骤 g)中 B 的消息后，A 执行下列步骤：

   1) 通过下列方式校验 $Token_{TA}$：验证包含在 $Token_{TA}$ 中 TP 的签名，检查在步骤 b)中发送给 TP 的随机数 R_A' 与包含在 $Token_{TA}$ 中被签名消息中的随机数 R_A' 是否一致。

   2) 从步骤 d)中 TP 发送的消息中提取 G' 的公钥，通过下列方式校验 $Token_{BA}$：验证包含在权标 $Token_{BA}$ 中的 B 的匿名签名，检查权标 $Token_{BA}$ 中被签名消息中的标识符域的值(G)与群组 G 的可区分标识符是否一致，检查包含在 $Token_{BA}$ 中被签名消息中的随机数 R_A 与在步骤 e)中发送给 B 的随机数 R_A 是否一致。

8.4 单向匿名双向鉴别

8.4.1 总则

单向匿名双向鉴别是指两个实体互相进行身份鉴别，其中一个实体对另外一个实体采用匿名鉴别。

8.4.2 机制 21——五次传递单向匿名双向鉴别(由实体 A 发起且 A 匿名)

在本机制中，属于群组 G 的实体 A 向实体 B 发起鉴别协议。惟一性或时效性通过产生并检查随机数(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。该鉴别机制如图 18 所示。

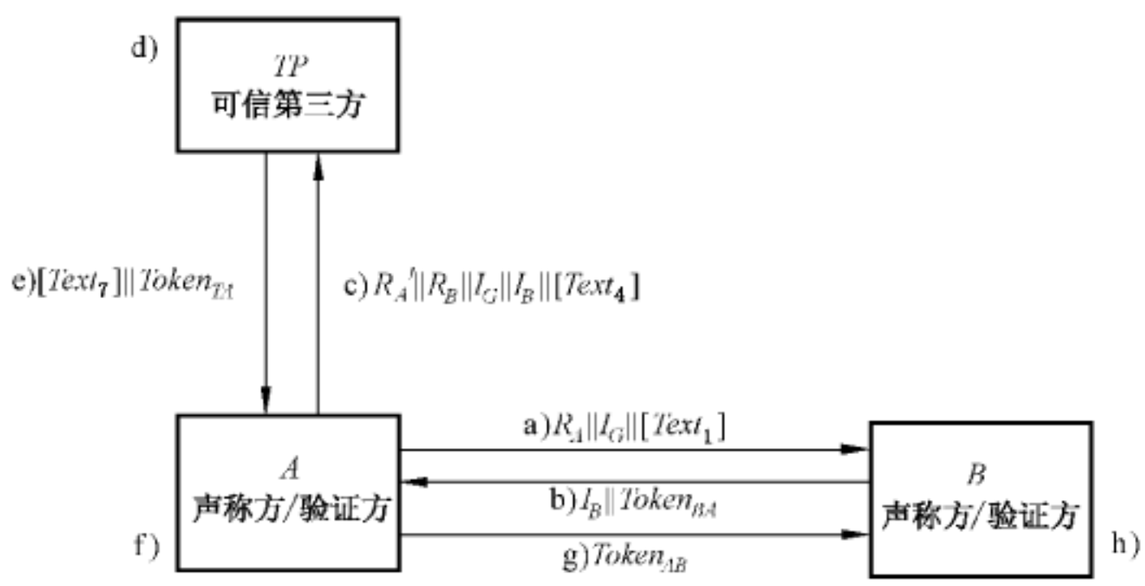

图 18 五次传递单向匿名双向鉴别(由 A 发起且 A 匿名)

权标应为如下两种形式。

选项 1：

$Token_{AB} = [Text_9] \| Res_G \| sS_T(R_B \| Res_G \| [Text_5]) \| gsS_{AG}(R_B \| R_A \| B \| G \| [Text_8])$；

$Token_{BA} = R_A \| R_B \| [Text_3] \| sS_B(B \| R_A \| R_B \| G \| [Text_2])$；

$Token_{TA}=Res_G \| Res_B \| sS_T(R_A' \| Res_B \| [Text_6]) \| sS_T(R_B \| Res_G \| [Text_5])$。

选项 2：

$Token_{AB}=R_A \| [Text_9] \| [Token_{TA} \| gsS_{AG}(R_B \| R_A \| B \| G \| [Text_8])$；

$Token_{BA}=R_A \| R_B \| [Text_3] \| sS_B(B \| R_A \| R_B \| G \| [Text_2])$；

$Token_{TA}=Res_G \| Res_B \| sS_T(R_A' \| R_B \| Res_G \| Res_B \| [Text_5])$。

字段 I_G，I_B，Res_G，Res_B 的值以及 *Status* 和 *Failure* 如下所示：

G：实体 A 所属的群组；

I_G：群组 G 的身份，为 G 或 $Cert_G$；

I_B：实体 B 的身份，为 B 或 $Cert_B$；

$Res_G=(Cert_G \| Status)$，$(G \| P_G)$或 *Failure*；

$Res_B=(Cert_B \| Status)$，$(B \| P_B)$或 *Failure*；

Status＝*True* 或 *False*。如果证书已经被撤消，则这个字段的值应为 *False*，否则这个字段应为 *True*；

Failure：当 *TP* 无法获得 G 的公钥或者证书，则 Res_G 字段的值应为 *Failure*。当 *TP* 无法获得 B 的公钥或者证书，则 Res_B 字段的值应为 *Failure*。

在本机制中，如果 *TP* 确认 G 身份和 P_G 之间的映射关系，则 $I_G=G$；否则，$I_G=Cert_G$，并且 G 应设置等于 $Cert_G$ 的可区分标识符字段值。如果 G 或者 $Cert_G$ 允许被用于作为一种身份，则应允许 *TP* 区分这两种类型的身份标识。Res_G 的值应按表 5 确定。

在本机制中，如果 *TP* 确认 B 身份和 P_B 之间的映射关系，则 $I_B=B$；否则，$I_B=Cert_B$，并且 B 应设置等于 $Cert_B$ 的可区分标识符字段值。如果 B 或者 $Cert_B$ 允许被用于作为一种身份，则宜允许 *TP* 区分这两种类型的身份标识。Res_B 的值应按表 6 确定。

表 5　Res_G 的值

字段	选项 1	选项 2
I_G	G	$Cert_G$
Res_G	$(G \| P_G)$或 *Failure*	$(Cert_G \| Status)$或 *Failure*

表 6　Res_B 的值

字段	选项 1	选项 2
I_B	B	$Cert_B$
Res_B	$(B \| P_B)$或 *Failure*	$(Cert_B \| Status)$或 *Failure*

本机制的执行过程如下：

a)　A 发送随机数 R_A、身份 I_G 和可选文本字段 $Text_1$ 到 B。

b)　B 发送 $Token_{BA}$ 和身份 I_B 到 A。

c)　A 发送随机数 R_A'、R_B，身份 I_G、I_B 和可选文本字段 $Text_4$ 到 *TP*。

d)　收到来自步骤 c)中 A 的消息后，*TP* 执行下列操作：如果 $I_G=G$，且 $I_B=B$，则 *TP* 提取 P_G 和 P_B；如果 $I_G=Cert_G$，且 $I_B=Cert_B$，则 *TP* 检查 $Cert_G$ 和 $Cert_B$ 的有效性。

e)　*TP* 发送 $Token_{TA}$ 和可选文本字段 $Text_7$ 到 A。$Token_{TA}$ 中的 Res_G 和 Res_B 字段应为 G 和 B 的证书及它们的状态，或者是 G 和 B 的可区分标识符及它们的公钥，或者是指示符 *Failure*。

f)　收到来自步骤 e)中 *TP* 的消息后，A 执行如下步骤：

1)　通过下列方式校验 $Token_{TA}$：验证包含在 $Token_{TA}$ 中 *TP* 的签名，检查在步骤 c)中发送给

TP 的随机数 R_A' 与包含在 $Token_{TA}$ 中 TP 的签名数据中的 R_A' 是否一致；

2） 通过检查 Res_B 验证 B 的有效性；

3） 从消息中提取 B 的公钥，通过下列方式校验 $Token_{BA}$：验证包含在 $Token_{BA}$ 中的 B 的签名，检查 $Token_{BA}$ 中被签名消息中的标识符域的值(G)与群组 G 的可区分标识符是否一致，检查包含在 $Token_{BA}$ 中的随机数 R_A 与在步骤 a)中发送给 B 的随机数 R_A 是否一致。

g） A 发送 $Token_{AB}$ 给 B。

h） 收到来自步骤 g)中 A 的消息后，B 执行下列步骤：

1） 通过下列方式校验 $Token_{TA}$：检查包含在 $Token_{TA}$ 中 TP 的签名，检查在步骤 b)中发送给 A 的随机数 R_B 与包含在 $Token_{TA}$ 中的签名数据中的 R_B 是否一致；

2） 通过检查 Res_G 验证 G 的有效性；

3） 从消息中提取 G 的公钥，通过下列方式校验 $Token_{AB}$：验证包含在权标 $Token_{AB}$ 中的 G 的群组签名，检查权标 $Token_{AB}$ 中被签名消息中的标识符域的值(B)与 B 的可区分标识符是否一致，检查包含在 $Token_{AB}$ 中的被签名消息中的随机数与在步骤 b)中发送给 G 的随机数 R_B 是否一致。

8.4.3 机制 22——五次传递单向匿名双向鉴别(由实体 *A* 发起且 *B* 匿名)

在本机制中，实体 A 向属于群组 G' 的实体 B 发起鉴别协议。惟一性或时效性通过产生并校验随机数(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。该鉴别机制如图 19 所示。

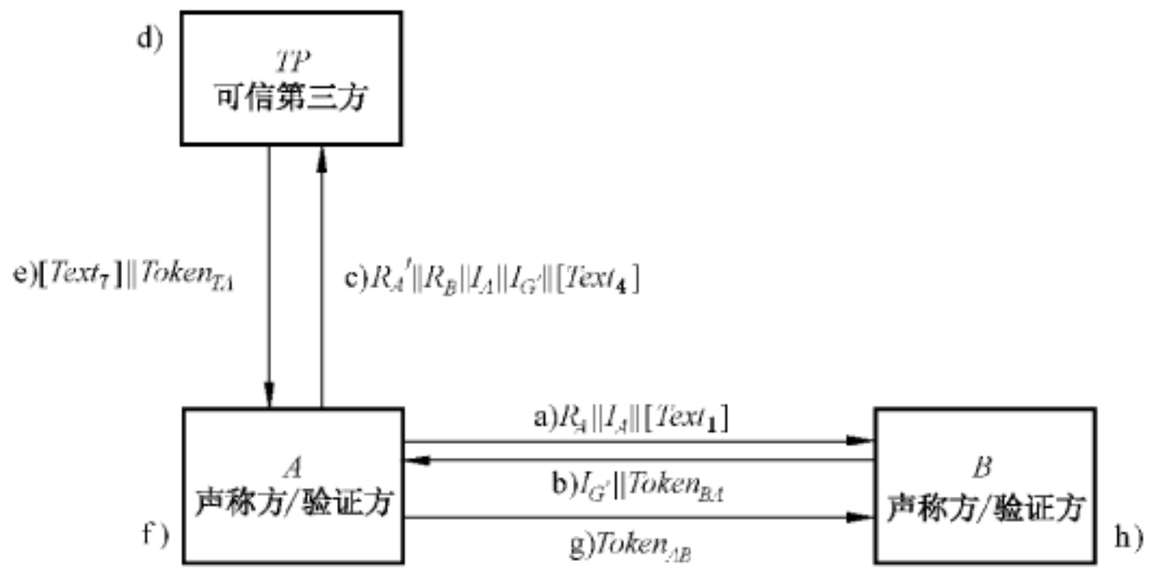

图 19 五次传递单向匿名双向鉴别(由 *A* 发起且 *B* 匿名)

权标应为如下两种形式。

选项 1：

$$Token_{AB}=[Text_9]\parallel Res_A\parallel sS_T(R_B\parallel Res_A\parallel[Text_5])\parallel sS_A(R_B\parallel R_A\parallel G'\parallel A\parallel[Text_8])；$$

$$Token_{BA}=R_A\parallel R_B\parallel[Text_3]\parallel gsS_{BG'}(G'\parallel R_A\parallel R_B\parallel A\parallel[Text_2])；$$

$$Token_{TA}=Res_A\parallel Res\,G'\parallel sS_T(R_A'\parallel Res_{G'}\parallel[Text_6])\parallel sS_T(R_B\parallel Res_A\parallel[Text_5])。$$

选项 2：

$$Token_{AB}=R_A\parallel[Text_9]\parallel Token_{TA}\parallel sS_A(R_B\parallel R_A\parallel G'\parallel A\parallel[Text_8])；$$

$$Token_{BA}=R_A\parallel R_B\parallel[Text_3]\parallel gsS_{BG'}(G'\parallel R_A\parallel R_B\parallel A\parallel[Text_2])；$$

$$Token_{TA}=Res_A\parallel Res_{G'}\parallel sS_T(R_A'\parallel R_B\parallel Res_A\parallel Res_{G'}\parallel[Text_5])。$$

字段 I_A，$I_{G'}$，Res_A，$Res_{G'}$ 的值以及 $Status$ 和 $Failure$ 如下所示：

G'：实体 B 所属的群组；

I_A：实体 A 的身份，为 A 或 $Cert_A$；

$I_{G'}$：群组 G' 的身份，为 G' 或 $Cert_{G'}$；

$Res_A=(Cert_A\parallel Status)$，$(A\parallel P_A)$ 或 $Failure$；

$Res_{G'}=(Cert_{G'}\parallel Status)$，$(G'\parallel P_{G'})$ 或 $Failure$；

$Status = True$ 或 $False$。如果证书已经被撤消，则这个字段的值应为 $False$，否则这个字段应为 $True$。

$Failure$：当 TP 无法获得 A 的公钥或者证书，则 Res_A 字段的值应为 $Failure$。当 TP 无法获得 G' 的公钥或者证书，则 $Res_{G'}$ 字段的值应为 $Failure$。

在本机制中，如果 TP 确认 A 身份和 P_A 之间的映射关系，则 $I_A = A$；否则，$I_A = Cert_A$，并且 A 应设置等于 $Cert_A$ 的可区分标识符字段值。如果 A 或者 $Cert_A$ 允许被用于作为一种身份，则宜允许 TP 区分这两种类型的身份标识。Res_A 的值应按表 7 确定。

在本机制中，如果 TP 确认 G' 身份和 $P_{G'}$ 之间的映射关系，则 $I_{G'} = G'$；否则，$I_{G'} = Cert_{G'}$，并且 G' 应设置等于 $Cert_{G'}$ 的可区分标识符字段值。如果 G' 或者 $Cert_{G'}$ 允许被用于作为一种身份，则宜允许 TP 区分这两种类型的身份标识。$Res_{G'}$ 的值应按表 8 确定。

表 7　Res_A 的值

字段	选项 1	选项 2
I_A	A	$Cert_A$
Res_A	$(A \parallel P_A)$或 $Failure$	$(Cert_A \parallel Status)$或 $Failure$

表 8　$Res_{G'}$ 的值

字段	选项 1	选项 2
$I_{G'}$	G'	$Cert_{G'}$
$Res_{G'}$	$(G' \parallel P_{G'})$或 $Failure$	$(Cert_{G'} \parallel Status)$或 $Failure$

本机制的执行过程如下：

a) A 发送随机数 R_A、身份 I_A 和可选文本字段 $Text_1$ 到 B。

b) B 发送 $Token_{BA}$ 和身份 $I_{G'}$ 到 A。

c) A 发送随机数 R_A'、R_B，身份 I_A、$I_{G'}$ 和可选文本字段 $Text_4$ 到 TP。

d) 收到来自步骤 c)中 A 的消息后，TP 执行下列操作：如果 $I_A = A$，且 $I_{G'} = G'$，则 TP 提取 P_A 和 $P_{G'}$；如果 $I_A = Cert_A$，且 $I_{G'} = Cert_{G'}$，则 TP 检查 $Cert_A$ 和 $Cert_{G'}$ 的有效性。

e) TP 发送 $Token_{TA}$ 和可选文本字段 $Text_7$ 到 A。$Token_{TA}$ 中的 Res_A 和 $Res_{G'}$ 字段应为 A 和 G' 的证书以及它们的状态，或者是 A 和 G' 的可区分标识符及它们的公钥，或者是指示符 $Failure$。

f) 收到来自步骤 e)中 TP 的消息后，A 执行如下步骤：

   1) 通过下列方式校验 $Token_{TA}$：验证包含在 $Token_{TA}$ 中 TP 的签名，检查在步骤 c)中发送给 TP 的随机数 R_A' 与包含在 $Token_{TA}$ 中的签名数据中的随机数 R_A' 是否一致；

   2) 通过检查 $Res_{G'}$ 验证 G' 的有效性；

   3) 从消息中提取 G' 的公钥，通过下列方式校验 $Token_{BA}$：验证包含在 $Token_{BA}$ 中的 B 的匿名签名，检查 $Token_{BA}$ 中被签名消息中的标识符域的值(A)与 A 的可区分标识符是否一致，检查包含在 $Token_{BA}$ 中的随机数 R_A 与在步骤 a)中发送给 B 的随机数 R_A 是否一致。

g) A 发送 $Token_{AB}$ 给 B。

h) 收到来自步骤 g)中 A 的消息后，B 执行下列步骤：

   1) 通过下列方式校验 $Token_{TA}$：验证包含在 $Token_{TA}$ 中 TP 的签名，检查在步骤 b)中发送给 A 的随机数 R_B 与包含在 $Token_{TA}$ 中的签名数据中的随机数 R_B 是否一致；

   2) 通过检查 Res_A 验证 A 的有效性；

3) 从消息中提取 A 的公钥，通过下列方式校验 $Token_{AB}$：验证包含在 $Token_{AB}$ 中的 A 的匿名签名，检查 $Token_{AB}$ 中的被签名消息中的标识符域的值(G')与群组 G' 的可区分标识符是否一致，检查包含在权标 $Token_{AB}$ 中的签名数据中的随机数 R_B 与在步骤 b)中发送给 A 的随机数 R_B 是否一致。

8.4.4 机制 23——五次传递单向匿名双向鉴别(由 *B* 发起且 *A* 匿名)

在本机制中，实体 B 向属于群组 G 的实体 A 发起鉴别协议。惟一性或时效性通过产生并检查随机数(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。该鉴别机制如图 20 所示。

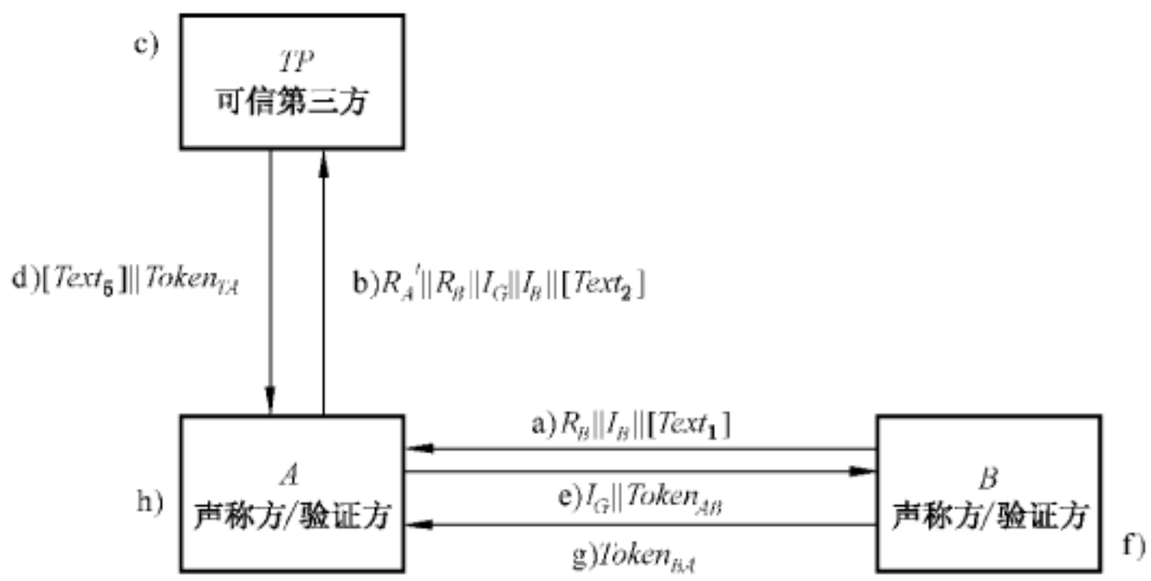

图 20 五次传递单向匿名双向鉴别(由 *B* 发起且 *A* 匿名)

权标应为如下两种形式。

选项 1：

$Token_{AB}=R_A \parallel [Text_7] \parallel Res_G \parallel sS_T(R_B \parallel Res_A \parallel [Text_3]) \parallel gsS_{AG}(R_B \parallel R_A \parallel B \parallel G \parallel [Text_6])$；

$Token_{BA}=R_A \parallel R_B \parallel [Text_9] \parallel sS_B(G \parallel R_A \parallel R_B \parallel B \parallel [Text_8])$；

$Token_{TA}=Res_G \parallel Res_B \parallel sS_T(R_A' \parallel Res_B \parallel [Text_4]) \parallel sS_T(R_B \parallel Res_G \parallel [Text_3])$。

选项 2：

$Token_{AB}=R_A \parallel [Text_7] \parallel Token_{TA} \parallel gsS_{AG}(R_B \parallel R_A \parallel B \parallel G \parallel [Text_6])$；

$Token_{BA}=R_A \parallel R_B \parallel [Text_9] \parallel sS_B(R_A \parallel R_B \parallel G \parallel B \parallel [Text_8])$；

$Token_{TA}=Res_G \parallel Res_B \parallel sS_T(R_A' \parallel R_B \parallel Res_G \parallel Res_B \parallel [Text_3])$。

字段 I_G，I_B，Res_G，Res_B 的值以及 $Status$ 和 $Failure$ 如下所示：

G：实体 A 所属的群组；

I_G：群组 G 的身份，为 G 或 $Cert_G$；

I_B：实体 B 的身份，为 B 或 $Cert_B$；

$Res_G=(Cert_G \parallel Status)$，$(G \parallel P_G)$或 $Failure$；

$Res_B=(Cert_B \parallel Status)$，$(B \parallel P_B)$或 $Failure$；

$Status=True$ 或 $False$。如果证书已经被撤消，则这个字段的值应为 $False$，否则这个字段应为 $True$。

$Failure$：当 TP 无法获得 G 的公钥或者证书，则 Res_G 字段的值应为 $Failure$。当 TP 无法获得 B 的公钥或者证书，则 Res_B 字段的值应为 $Failure$。

在本机制中，如果 TP 确认 G 身份和 P_G 之间的映射关系，则 $I_G=G$；否则，$I_G=Cert_G$，并且 G 应设置等于 $Cert_G$ 的可区分标识符字段值。如果 G 或者 $Cert_G$ 允许被用于作为一种身份，则宜允许 TP 区分这两种类型的身份标识。Res_G 的值应按表 9 确定。

在本机制中，如果 TP 确认 B 身份和 P_B 之间的映射关系，则 $I_B=B$；否则，$I_B=Cert_B$，并且 B 应设置等于 $Cert_B$ 的可区分标识符字段值。如果 B 或者 $Cert_B$ 允许被用于作为一种身份，则宜允许 TP

区分这两种类型的身份标识。Res_B 的值应按表 10 确定。

表 9　Res_G 的值

字段	选项 1	选项 2
I_G	G	$Cert_G$
Res_G	$(G \parallel P_G)$或 $Failure$	$(Cert_G \parallel Status)$或 $Failure$

表 10　Res_B 的值

字段	选项 1	选项 2
I_B	B	$Cert_B$
Res_B	$(B \parallel P_B)$或 $Failure$	$(Cert_B \parallel Status)$或 $Failure$

本机制的执行过程如下：

a)　B 发送随机数 R_B、身份 I_B 和可选文本字段 $Text_1$ 到 A。

b)　A 发送随机数 R_A'、R_B，身份 I_G、I_B 和可选文本字段 $Text_2$ 到 TP。

c)　收到来自步骤 b)中 A 的消息后，TP 执行下列操作：如果 $I_G=G$，且 $I_B=B$，则 TP 提取 P_G 和 P_B；如果 $I_G=Cert_G$，且 $I_B=Cert_B$，则 TP 检查 $Cert_G$ 和 $Cert_B$ 的有效性。

d)　TP 发送 $Token_{TA}$ 和可选文本字段 $Text_5$ 到 A。$Token_{TA}$ 中的 Res_G 和 Res_B 字段应为 G 和 B 的证书及它们的状态，或者是 G 和 B 的可区分标识符和它们的公钥，或者是指示符 $Failure$。

e)　A 发送权标 $Token_{AB}$ 和身份 I_G 到 B。

f)　收到来自步骤 e)中 A 的消息后，B 执行下列步骤：

　1)　通过下列方式验证 $Token_{AB}$ 中 TP 的签名：检查在步骤 a)中发送给 A 的随机数 R_B 与包含在权标 $Token_{AB}$ 中 TP 的签名数据中的随机数 R_B 是否一致；

　2)　通过检查 Res_G 验证 G 的有效性；

　3)　从消息中提取 G 的公钥，通过下列方式校验 $Token_{AB}$：验证包含在权标 $Token_{AB}$ 中的 A 的匿名签名，检查权标 $Token_{AB}$ 中被签名消息中的标识符域的值(B)与 B 的可区分标识符是否一致，检查包含在权标 $Token_{AB}$ 中 A 的签名数据中的随机数 R_B 与在步骤 a)中发送给 A 的随机数 R_B 是否一致。

g)　B 发送 $Token_{BA}$ 到 A。

h)　收到来自步骤 g)中 B 的消息后，A 执行下列步骤：

　1)　通过下列方式校验 $Token_{TA}$：验证包含在 $Token_{TA}$ 中 TP 的签名，检查在步骤 b)中发送给 TP 的随机数 R_A' 与包含在 $Token_{TA}$ 中的签名数据中的随机数 R_A' 是否一致；

　2)　通过检查 Res_B 验证 B 的有效性；

　3)　从步骤 d)中 TP 发送的消息中提取 B 的公钥，通过下列方式校验 $Token_{BA}$：检查包含在 $Token_{BA}$ 中的 B 的匿名签名，检查 $Token_{BA}$ 中被签名消息中的标识符域的值(G)与群组 G 的可区分标识符是否一致，检查包含在 $Token_{BA}$ 中的签名数据中的随机数 R_A 与在步骤 e)中发送给 B 的随机数 R_A 是否一致。

8.4.5　机制 24——五次传递单向匿名双向鉴别(由 *B* 发起且 *B* 匿名)

在本机制中，实体 B 向属于群组 G 的实体 A 发起鉴别协议。惟一性或时效性通过产生并校验随机数(参见 ISO/IEC 9798-1:2010[3]的附录 B)来控制。该鉴别机制如图 21 所示。

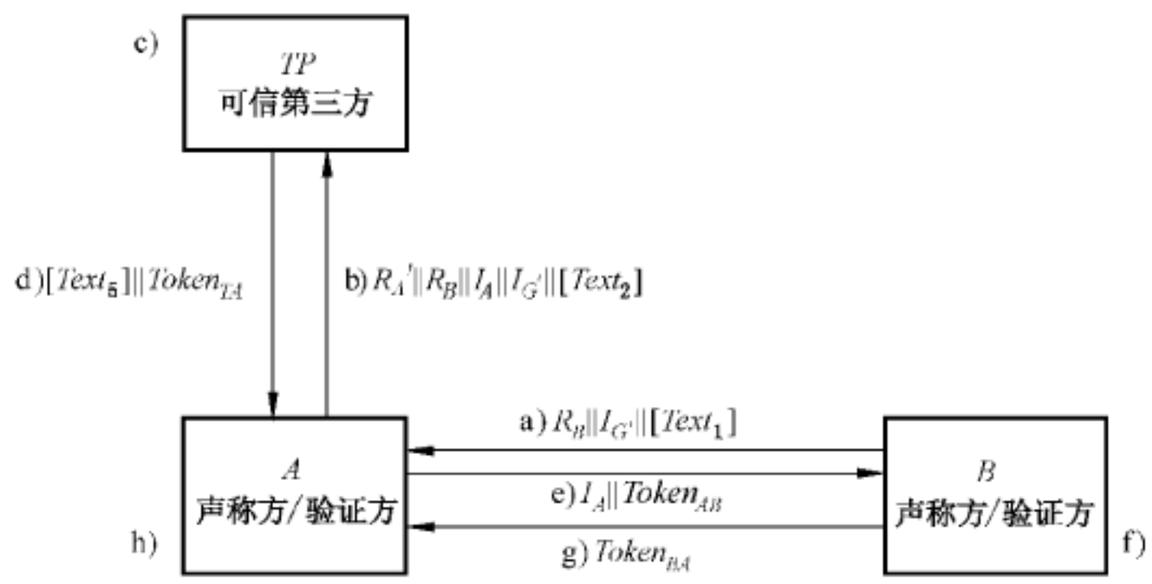

图 21　五次传递单向匿名双向鉴别(由 *B* 发起且 *B* 匿名)

权标应为如下两种形式。

选项 1:

$Token_{AB}=[Text_7]\parallel R_A\parallel Res_A\parallel sS_T(R_B\parallel Res_A\parallel[Text_3])\parallel sS_A(R_B\parallel R_A\parallel G'\parallel A\parallel[Text_6])$;

$Token_{BA}=R_A\parallel R_B\parallel[Text_9]\parallel gsS_{BG'}(A\parallel R_A\parallel R_B\parallel G'\parallel[Text_8])$;

$Token_{TA}=Res_A\parallel Res_{G'}\parallel sS_T(R_A'\parallel Res_{G'}\parallel[Text_4])\parallel sS_T(R_B\parallel Res_A\parallel[Text_3])$。

选项 2:

$Token_{AB}=R_A\parallel[Text_7]\parallel Token_{TA}\parallel sS_A(R_B\parallel R_A\parallel G'\parallel A\parallel[Text_6])$;

$Token_{BA}=R_A\parallel R_B\parallel[Text_9]\parallel gsS_{BG'}(R_A\parallel R_B\parallel A\parallel G'\parallel[Text_8])$;

$Token_{TA}=Res_A\parallel Res_{G'}\parallel sS_T(R_A'\parallel R_B\parallel Res_A\parallel Res_{G'}\parallel[Text_3])$。

字段 I_A,$I_{G'}$,Res_A,$Res_{G'}$ 的值以及 *Status* 和 *Failure* 如下所示:

G':实体 B 所属的群组;

I_A:实体 A 的身份,可以为 A 或者 $Cert_A$;

$I_{G'}$:群组 G' 的身份,可以为 G' 或者 $Cert_{G'}$;

$Res_A=(Cert_A\parallel Status)$,$(A\parallel P_A)$ 或 *Failure*;

$Res_{G'}=(Cert_{G'}\parallel Status)$,$(G'\parallel P_{G'})$ 或 *Failure*;

Status=*True* 或 *False*。如果证书已经被取消,则这个字段的值应设置为 *False*,否则这个字段应设置为 *True*;

Failure:当 *TP* 无法获得 A 的公钥或者证书,则 Res_A 字段的值应为 *Failure*。当 *TP* 无法获得 G' 的公钥或者证书,则 $Res_{G'}$ 字段的值应为 *Failure*。

在本机制中,如果 *TP* 确认 A 身份和 P_A 之间的映射关系,则 $I_A=A$;否则,$I_A=Cert_A$,并且 A 应设置等于 $Cert_A$ 的可区分标识符字段值。如果 A 或者 $Cert_A$ 允许被用于作为一种身份,则宜允许 *TP* 区分这两种类型的身份标识。Res_A 的值应按表 11 确定。

在本机制中,如果 *TP* 确认 G' 身份和 $P_{G'}$ 之间的映射关系,则 $I_{G'}=G'$;否则,$I_{G'}=Cert_{G'}$,并且 G' 应设置等于 $Cert_{G'}$ 的可区分标识符字段值。如果 G' 或者 $Cert_{G'}$ 允许被用于作为一种身份,则宜允许 *TP* 区分这两种类型的身份标识。$Res_{G'}$ 的值应按表 12 确定。

表 11 Res_A 的值

字段	选项 1	选项 2
I_A	A	$Cert_A$
Res_A	$(A \parallel P_A)$或 $Failure$	$(Cert_A \parallel Status)$或 $Failure$

表 12 $Res_{G'}$ 的值

字段	选项 1	选项 2
$I_{G'}$	G'	$Cert_{G'}$
$Res_{G'}$	$(G' \parallel P_{G'})$或 $Failure$	$(Cert_{G'} \parallel Status)$或 $Failure$

本机制的执行过程如下：

a) B 发送随机数 R_B、身份 $I_{G'}$ 和可选文本字段 $Text_1$ 到 A。

b) A 发送随机数 $R_A{}'$、R_B，身份 I_A、$I_{G'}$ 和可选文本字段 $Text_2$ 到 TP。

c) 收到来自步骤 b)中 A 的消息后，TP 执行下列操作：如果 $I_A=A$，且 $I_{G'}=G'$，则 TP 提取 P_A 和 $P_{G'}$；如果 $I_A=Cert_A$，且 $I_{G'}=Cert_{G'}$，则 TP 检查 $Cert_A$ 和 $Cert_{G'}$ 的有效性。

d) TP 发送 $Token_{TA}$ 和可选文本字段 $Text_5$ 到 A。$Token_{TA}$ 中的 Res_A 和 $Res_{G'}$ 字段应为 A 和 G' 的证书及它们的状态，或者是 A 和 G' 的可区分标识符和它们的公钥，或者是指示符 $Failure$。

e) A 发送权标 $Token_{AB}$ 和身份 I_A 到 B。

f) 收到来自步骤 e)中 A 的消息后，B 执行下列步骤：

   1) 通过下列方式验证 $Token_{AB}$ 中 TP 的签名：检查在步骤 a)中发送给 A 的随机数 R_B 与包含在权标 $Token_{AB}$ 中 TP 的签名数据中的随机数 R_B 是否一致；

   2) 通过检查 Res_A 验证 A 的有效性；

   3) 从消息中提取 A 的公钥，通过下列方式校验 $Token_{AB}$：验证包含在权标 $Token_{AB}$ 中的 A 的匿名签名，检查权标 $Token_{AB}$ 中被签名消息中的标识符域的值(G')与群组 G' 的可区分标识符是否一致，检查包含在权标 $Token_{AB}$ 中 A 的签名数据中的随机数 R_B 与在步骤 a)中发送给 A 的随机数 R_B 是否一致。

g) B 发送 $Token_{BA}$ 到 A。

h) 收到来自步骤 g)中 B 的消息后，A 执行下列步骤：

   1) 通过下列方式校验 $Token_{TA}$：检查在步骤 b)中发送给 TP 的随机数 $R_A{}'$ 与包含在 $Token_{BA}$ 中的签名数据中的 $R_A{}'$ 是否一致；

   2) 通过检查 $Res_{G'}$ 验证 G' 的有效性；

   3) 从步骤 d)中 TP 发送的消息中提取 G' 的公钥，通过下列方式校验 $Token_{BA}$：检查包含在权标 $Token_{BA}$ 中的 B 的匿名签名，检查权标 $Token_{BA}$ 中已签信息中的标识符域的值(A)与群组 A 的可区分标识符是否一致，检查包含在权标 $Token_{BA}$ 中的签名数据中的随机数 R_A 与在步骤 e)中发送给 B 的随机数 R_A 是否一致。

9 群组成员打开过程

9.1 总则

该过程是可选的。如果群组签名机制支持打开，打开过程则存在。打开者拥有打开密钥，才允许该过程执行。群组成员打开的目的是为了区分出不同的参与群组签名的实体的可区分标识符。如果一个

匿名鉴别支持打开过程，该过程称为部分匿名鉴别。

注：关于打开过程的信息包含在文本字段中。

本部分给出了群组成员的打开过程。

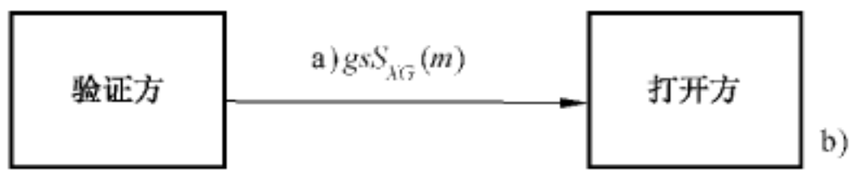

图 22　打开过程

打开过程如图 22 描述所示。其中，输入包括群组签名、该群组成员打开密钥、群组公钥和群组公共参数，该过程返回一个可区分标识符，同时也可以返回一个绑定证据。

打开过程包含：

a)　验证方发送从群组 G 中 X 成员收到的匿名的群组签名 $gsS_{XG}(m)$给打开方。

b)　打开方使用群组成员打开密钥找出一个可区分标识符，同时也可输出一个绑定证据。

9.2　证据评价过程

该过程是可选的。证据评价过程运行在证据评价者上，其作用是检查提供的签名是否是由特定的签名方产生。

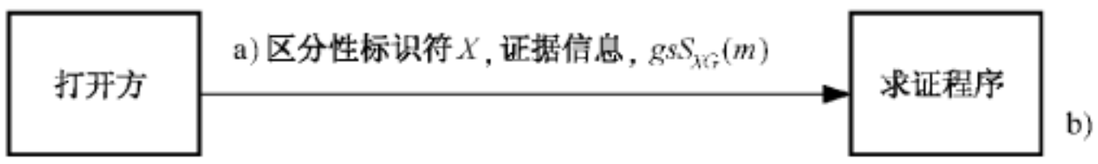

图 23　证据评价过程

该过程包含了步骤 a)和 b)，如图 23 所示。它将绑定证据、群组签名和可区分标识符作为输入，并且返回签名方的有效性。

a)　打开方发送可区分标识符 X、绑定证据和从群组 G 中成员 X 收到的匿名的群组签名 $gsS_{XG}(m)$给证据评价者；

b)　证据评价者确定这些证据的有效性。

10　群组签名连接过程

10.1　总则

连接过程运行在群组的连接方上，该过程允许连接多个由相同的签名者产生的群组签名。

这个过程是可选的。用于连接方确定给定的群签名是否来自同一个匿名用户。如果给定的群组签名来自于相同的匿名用户，则群组签名可连接，否则签名不可连接。

注：关于连接过程的信息包含在文本字段中。

10.2　与打开方的连接过程

针对该过程，群组签名宜支持打开能力，打开方通过其可识别群组签名的签名者，该过程包括打开方通知连接方两个群组签名是否连接。

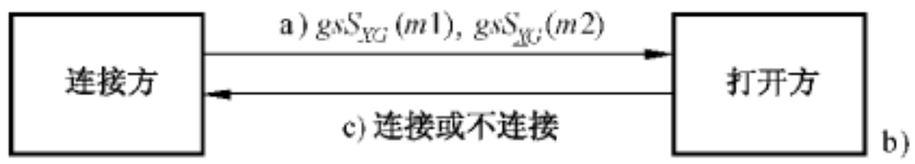

图 24　与打开方的连接过程

该过程包含了步骤 a)～c)，如图 24 所示，该过程在鉴别过程后执行，处理过程如下：

a)　连接方发送 $gsS_{XG}(m1)$、$gsS_{\underline{X}G}(m2)$给打开方，实体 X 和 $\underline{X}$ 可能是相同的实体；

b)　打开方通过比较群组签名的可区分标识符来检查这两个用来鉴别的群组签名是否来自于相同的声称方；

c)　打开方对群组签名是否可以连接做出响应。

10.3　带有连接密钥的连接过程

针对该过程，群组签名方案宜具有连接方能够决定提供的群组签名是否可以连接的能力，且该过程没有打开方参与。

在该过程中，验证方宜是连接方，连接方应拥有一个连接密钥和具备本地连接的能力。

通过该过程，连接方可以判断给定的两部分群组签名是否可以使用连接密钥进行连接。

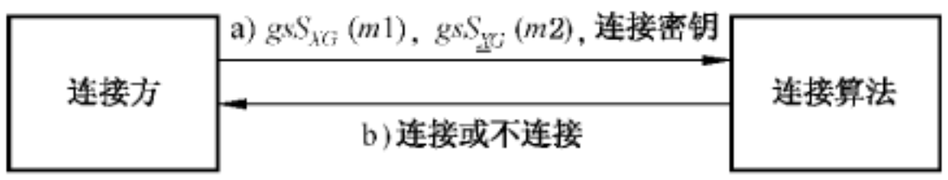

图 25　与连接密钥的连接过程

该过程包含了步骤 a)和 b)，如图 25 所示。该过程在鉴别过程后执行，处理过程如下：

a)　连接方调用连接算法，其中 $gsS_{XG}(m1)$、$gsS_{\underline{X}G}(m2)$、连接密钥和群组公共参数作为输入，实体 X 和 $\underline{X}$ 可能是相同的实体；

b)　连接算法向连接方输出群组签名是否是连接的。

10.4　带有连接库的连接过程

针对该过程，群组签名方案宜具备有连接能力，使用一个连接库时签名者生成的签名实现连接，而不同的签名者或者使用不同的连接库则不能实现该连接过程。在匿名实体鉴别协议中，为了拥有此连接能力，验证方应发送连接库给声称方作为可选文本。声称方使用连接库和群组私钥生成群组签名。连接算法不依赖任何连接密钥，并且任何实体都能执行连接算法。通过此连接过程，连接方能知道给定的两对或多对群组签名是否是连接的。

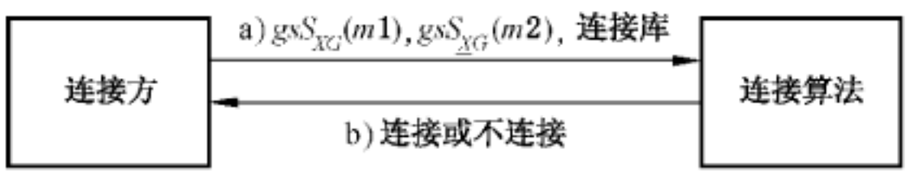

图 26　与连接库的连接过程

该过程包含了步骤 a)和 b)，如图 26 所示。该过程在鉴别过程后执行，处理过程如下：

a)　连接方调用连接算法，其中 $gsS_{XG}(m1)$、$gsS_{\underline{X}G}(m2)$、连接库和群组公共参数作为输入，实体 X 和 $\underline{X}$ 可能相同；

b)　连接算法向连接方输出群组签名是否是连接的。

附 录 A
（规范性附录）
对象标识符

本附录列出了本部分中分配给匿名鉴别机制的对象标识符。

```
AnonymousEntityAuthenticationMechanisms-2 {
iso(1)standard(0)anonymous-entity-authentication-mechanisms(20009)part2 (2)
asn1-module(0)object-identifiers(0)}
DEFINITIONS EXPLICIT TAGS ::= BEGIN
-- EXPORTS All; --
-- IMPORTS None; --
OID ::= OBJECT IDENTIFIER- alias
-- Synonyms--
Is20009-2 OID ::= { iso(1)standard(0)anonymous-entity-authentication-mechanisms
(20009)part2(2)}
mechanism OID ::= { is20009-2 mechanisms(2)}
-- mechanisms not involving a trusted third party--
anony-ua-one-pass OID ::= { mechanism 1 }
anony-ua-two-pass OID ::= { mechanism 2 }
anony-ma-two-pass OID ::= { mechanism 3 }
anony-ma-three-pass OID ::= { mechanism 4 }
anony-ma-two-pass-Parallel OID ::= { mechanism 5 }
uni-anony-ma-two-pass OID ::= { mechanism 6 }
uni-anony-ma-three-pass OID ::= { mechanism 7 }
uni-anony-ma-two-pass-Parallel OID ::= { mechanism 8 }
anony-ma-three-pass-bind-sig-later OID ::= { mechanism 9 }
anony-ma-three-pass-bind-sig-first OID ::= { mechanism 10 }
anony-ma-two-pass-Parallel-bind-sig-later OID ::= { mechanism 11 }
anony-ma-two-pass-Parallel-bind-sig-first OID ::= { mechanism 12 }
anony-uni-anony-ma-three-pass-bind-sig-later OID ::= { mechanism 13 }
anony-uni-anony-ma-three-pass-bind-sig-first OID ::= { mechanism 14 }
anony-uni-anony-ma-two-pass-Parallel-bind-sig-later OID ::= { mechanism 15 }
anony-uni-anony-ma-two-pass-Parallel-bind-sig-first OID ::= { mechanism 16 }
-- mechanisms involving a trusted third party--
ttp-anony-ua-four-pass-by-A OID ::= { mechanism 17 }
ttp-anony-ua-four-pass-by-B OID ::= { mechanism 18 }
ttp-anony-ma-five-pass-by-A OID ::= { mechanism 19 }
ttp-anony-ma-five-pass-by-B OID ::= { mechanism 20 }
ttp-uni-anony-ma-five-pass-by-A-A OID ::= { mechanism 21 }
ttp-uni-anony-ma-five-pass-by-A-B OID ::= { mechanism 22 }
ttp-uni-anony-ma-five-pass-by-B-A OID ::= { mechanism 23 }
ttp-uni-anony-ma-five-pass-by-B-B OID ::= { mechanism 24 }
END -- AnonymousEntityAuthenticationMechanisms-2-
```

附　录　B
（资料性附录）
具有绑定属性的机制的信息

本附录解释了在一些特定环境中使用绑定属性的必要性以及包含参数选择的指导。

首先，关于误绑定攻击的 3 个例子描述如下：

示例 1：

在 7.3.3 的机制 4 中，实体 B 向实体 A 通过发送消息 $R_B \| [Text_1]$ 发起鉴别协议。实体 A 使用消息 $[Cert_G] \| Token_{AB}$ 进行响应。现在另外一个和实体 B 在相同群组中的实体 B' 能够产生消息 $[Cert_{G'}] \| Token_{BA}$ 发送给实体 A 且没有被侦测出来。因此，实体 A 鉴别出了是实体 B' 而不是实体 B 发起了鉴别协议。

示例 2：

在 7.3.4 的机制 5 中，实体 A 发送消息 $R_A \| [Cert_G] \| [Text_1]$ 给实体 B，与此同时，实体 B 发送消息 $R_B \| [Cert_{G'}] \| [Text_2]$ 给实体 A，现在另外一个和实体 B 在相同群组中的实体 B' 能够产生信息 $Token_{BA}$ 发送给实体 A 且没有被侦测出来。因此，实体 A 鉴别出是实体 B' 而不是实体 B 发送了该协议的第一条消息。

示例 3：

在 7.3.3 的机制 4 中，群组 G' 中的实体 B 通过发送信息 $R_B \| [Text_1]$ 向实体 A 发起鉴别协议。实体 A 对信息 $[Cert_G] \| Token_{AB}$ 进行响应。如果 $Token_{AB}$ 中没有包含 G'，那时，另外一个群组 G'' 中的实体 B' 就能够替换最后的消息并发送 $[Cert_{G''}] \| Token_{BA}$ 给实体 A 且没有被侦测出来。因此，实体 A 鉴别出是实体 B' 而不是实体 B 发起的鉴别协议。

在以上例子中，当协议结束，实体 B 鉴别出实体 A，而实体 A 却鉴别出了替换实体 B 发送了第一条信息的另外一个实体 B'。在上面的最后一个例子中，实体可能认为实体 B 发送的任何信息（基于地址或者 B 的位置）就是来自于群组 G'' 中成员。然而，事实上实体 B 却属于群组 G'，这种误绑定攻击改变了鉴别协议的完整性。由于实体发送的协议消息之间是没有绑定的，因而这种攻击是可能的。

在机制 4 中的其他形式误绑定攻击如下：

示例 4：

在机制 4 中，实体 B 通过发送信息 $R_B \| [Text_1]$ 向 A 发起鉴别协议，实体 A 通过信息 $[Cert_G] \| Token_{AB}$ 进行响应，实体 B 发送 $[Cert_{G'}] \| Token_{BA}$ 作为最后一条消息。现在另外一个和实体 B 属于同一群组的实体 B' 能够拦截这条最后一条消息并且使用它自己的签名替换 $Token_{BA}$ 中的群组签名 $gsS_{BG'}(R_B \| R_A \| [G] \| [Text_4])$。最后，鉴别协议成功。然而，实体 A 使用实体 B' 的签名鉴别出了实体 B。由于实体 A 能够立即侦测出这种替换，因而这种攻击在使用传统签名的传统鉴别机制中是不可能的。

在上述例子中，误绑定攻击也许并不是一个问题，因为实体 A 并不关心鉴别出的是实体 B 还是实体 B'，实体 A 也许仅仅关心是否鉴别出了群组 G' 中的一个成员。然而，在一些使用场景中，这种误绑定攻击需要被关注，例如，在鉴别协议中使用的匿名数字签名具有打开能力，实体 A 也许会周期的发送它所收集到的全部群组签名给打开方。如果被允许，实体 A 可以获得一些统计，例如，一个实体被鉴别了多少次。实体 A 可以获得在这种误绑定攻击下的全部错误统计。

实体鉴别协议的绑定属性是一种确保一个交互实体所有的信息都被绑定在一起的属性，如果这些信息中的一个或者一部分被篡改或重放，这种变动能够被协议侦测出来。因此，绑定属性在鉴别协议的完整性上提供了高可靠性。一般情况下，为了获得绑定属性，需要使用到 Diffie-Hellman 密钥管理技术。使用 Diffie-Hellman 的目标不是为了两个实体之间的密钥管理，而是为了确保协议信息的完整性。

在 7.5 和 7.6 这些带有绑定属性的机制中，阶 q 在循环群 G 上的 DDH 问题是困难的，实体 A 和实体 B 选择群 G 中的生成元 g，两个选择循环群 G 和 g 的例子如下所示：

——传统机制：选择大素数 p 和 q，使得 $p-1$ 是 q 的倍数。循环群 G 是被定义为 Z_p* 上的 q 阶子群。选择一个数 g，该数对 p 求模的结果是 q（更多信息请参考 ISO/IEC 11770-3 [6]）。然后，在 7.5 和 7.6 的机制中去计算 g^a 和 $g^a \bmod p$。

——基于椭圆曲线的机制：选择一个素数 q 阶的椭圆群 G 和一个生成点 g（更多关于椭圆曲线的信息请参考 ISO/IEC 15946-1[7]）。然后，在 7.5 和 7.6 的机制中计算 g^a 和点乘运算 $[a]g$。

参 考 文 献

[1] ISO/IEC 8825-1:2008 Information technology—ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)—Part 1

[2] ISO/IEC 9797-1:2011 Information technology—Security techniques—Message Authentication Codes (MACs)—Part 1: Mechanisms using a block cipher

[3] ISO/IEC 9798-1:2010 Information technology—Security techniques—Entity authentication—Part 1: General

[4] ISO/IEC 9798-3:1998 Information technology—Security techniques—Entity authentication—Part 3: Mechanisms using digital signaTrue techniques

[5] ISO/IEC 11770-1:2010 Information technology—Security techniques—Key management—Part 1: Framework

[6] ISO/IEC 11770-3:2008 Information technology—Security techniques—Key management—Part 3: Mechanisms using asymmetric techniques

[7] ISO/IEC 15946-1:2008 Information technology—Security techniques—Cryptographic techniques based on elliptic curves—Part 1: General

[8] Brickell E., & Li J.A pairing-based DAA scheme further reducing TPM resources, TRUST 2010(LNCS 6101), pp.181-195, 2010.

[9] Hwang J., Lee S., Chung B., Cho H., Nyang D.Short Group SignaTrues with Controllable Linkability.LIGHTSEC.2011, 2011 pp.44-52.

[10] Hwang J., Eom S., Chang K., Lee P., Nyang D.Anonymity-based authenticated key agreement with binding properties.WISA.2012, 2012 pp.177-191.

[11] Walker J., & Li J.Key Exchange with Anonymous Authentication using DAA-SIGMA Protocol, Proc.of 2nd International Conference on Trusted Systems (LNCS 6802), pp.108-127, 2010.

GB/T 34953.2—2018/ISO/IEC 20009-2:2013

中 华 人 民 共 和 国
国 家 标 准
信息技术 安全技术 匿名实体鉴别
第 2 部分:基于群组公钥签名的机制
GB/T 34953.2—2018/ISO/IEC 20009-2:2013
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2018 年 9 月第一版
*
书号:155066·1-61359

版权专有 侵权必究

GB/T 34953.2-2018