ICS 35.040
L 80
备案号：55615—2016

GM

中华人民共和国密码行业标准

GM/T 0044.3—2016

SM9 标识密码算法 第 3 部分：密钥交换协议

Identity-based cryptographic algorithms SM9—Part 3：Key exchange protocol

2016-03-28 发布　　2016-03-28 实施

国家密码管理局　　发布

目　　次

前　言

GM/T 0044《SM9 标识密码算法》分为 5 个部分：

——第 1 部分：总则；

——第 2 部分：数字签名算法；

——第 3 部分：密钥交换协议；

——第 4 部分：密钥封装机制和公钥加密算法；

——第 5 部分：参数定义。

本部分为 GM/T 0044 的第 3 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分由密码行业标准化技术委员会提出并归口。

本部分起草单位：国家信息安全工程技术研究中心、深圳奥联信息安全技术有限公司、武汉大学、上海交通大学、中科院信息工程研究所、北方信息技术研究所。

本部分主要起草人：陈晓、程朝辉、叶顶峰、胡磊、陈建华、路贝可、季庆光、曹珍富、袁文恭、刘平、马宁、袁峰、李增欣、王学进、杨恒亮、张青坡、马艳丽、浦雨三、唐英、孙移盛、安萱。

引　言

A.Shamir 在 1984 年提出了标识密码(Identity-Based Cryptography)的概念，在标识密码系统中，用户的私钥由密钥生成中心(KGC)根据主密钥和用户标识计算得出，用户的公钥由用户标识唯一确定，从而用户不需要通过第三方保证其公钥的真实性。与基于证书的公钥密码系统相比，标识密码系统中的密钥管理环节可以得到适当简化。

1999 年，K.Ohgishi、R.Sakai 和 M.Kasahara 在日本提出了用椭圆曲线对(pairing)构造基于标识的密钥共享方案；2001 年，D.Boneh 和 M.Franklin，以及 R.Sakai、K.Ohgishi 和 M.Kasahara 等人独立提出了用椭圆曲线对构造标识公钥加密算法。这些工作引发了标识密码的新发展，出现了一批用椭圆曲线对实现的标识密码算法，其中包括数字签名算法、密钥交换协议、密钥封装机制和公钥加密算法等。

椭圆曲线对具有双线性的性质，它在椭圆曲线的循环子群与扩域的乘法循环子群之间建立联系，构成了双线性 DH、双线性逆 DH、判定性双线性逆 DH、τ-双线性逆 DH 和 τ-Gap-双线性逆 DH 等难题，当椭圆曲线离散对数问题和扩域离散对数问题的求解难度相当时，可用椭圆曲线对构造出安全性和实现效率兼顾的标识密码。

本部分描述了用椭圆曲线对实现的基于标识的密钥交换协议。

SM9 标识密码算法
第 3 部分:密钥交换协议

1 范围

GM/T 0044 的本部分规定了用椭圆曲线对实现的基于标识的密钥交换协议,并提供了相应的流程。该协议可以使通信双方通过对方的标识和自身的私钥经两次或可选三次信息传递过程,计算获取一个由双方共同决定的共享秘密密钥。该秘密密钥可作为对称密码算法的会话密钥。协议中选项可以实现密钥确认。

本部分适用于密钥管理与协商。

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。

GM/T 0004—2012 SM3 密码杂凑算法

GM/T 0044.1—2016 SM9 标识密码算法 第 1 部分:总则

GM/T 0044.2—2016 SM9 标识密码算法 第 2 部分:数字签名算法

3 术语和定义

下列术语和定义适用于本文件。

3.1

密钥交换 key exchange

在通信实体之间安全地交换密钥的方案,可以使通信双方在非安全通信线路上为信息传送安全地交换密钥。

3.2

密钥协商 key agreement

多个用户之间建立一个共享秘密密钥的过程,并且其中的任何一个用户都不能预先确定该密钥的值。

3.3

从 A 到 B 的密钥确认 key confirmation from A to B

使用户 B 确信用户 A 拥有特定秘密密钥的保证。

3.4

密钥派生函数 key derivation function

通过作用于共享秘密和双方都知道的其他参数,产生一个或多个共享秘密密钥的函数。

3.5

发起方 initiator

在一个协议的操作过程中发送首轮交换信息的用户。

3.6

响应方　responder

在一个协议的操作过程中不是发送首轮交换信息的用户。

3.7

加密主密钥　encryption master key

处于标识密码密钥分层结构最顶层的密钥，包括加密主私钥和加密主公钥，其中加密主公钥公开，加密主私钥由 KGC 秘密保存。KGC 用加密主私钥和用户的标识生成用户的加密私钥。在标识密码中，加密主私钥一般由 KGC 通过随机数发生器产生，加密主公钥由加密主私钥结合系统参数产生。

3.8

标识　identity

可唯一确定一个实体身份的信息。标识应由实体无法否认的信息组成，如实体的可识别名称、电子邮箱、身份证号、电话号码、街道地址等。

3.9

密钥生成中心　key generation center；KGC

在本部分中，负责选择系统参数、生成加密主密钥并产生用户加密私钥的可信机构。

4　符号

下列符号适用于本文件。

A，B：使用公钥密码系统的两个用户。

cf：椭圆曲线阶相对于 N 的余因子。

cid：用一个字节表示的曲线的识别符，其中 0x10 表示 F_p（素数 $p>2^{191}$）上常曲线（即非超奇异曲线），0x11 表示 F_p 上超奇异曲线，0x12 表示 F_p 上常曲线及其扭曲线。

de_A：用户 A 的加密私钥。

de_B：用户 B 的加密私钥。

e：从 $G_1 \times G_2$ 到 G_T 的双线性对。

eid：用一个字节表示的双线性对 e 的识别符，其中 0x01 表示 Tate 对，0x02 表示 Weil 对，0x03 表示 Atc 对，0x04 表示 R-ate 对。

G_T：阶为素数 N 的乘法循环群。

G_1：阶为素数 N 的加法循环群。

G_2：阶为素数 N 的加法循环群。

g^u：乘法群 G_T 中元素 g 的 u 次幂，即 $g^u = \underbrace{g \cdot g \cdot \ldots \cdot g}_{u个}$，$u$ 是正整数。

$H_v(\ )$，$Hash(\ )$：密码杂凑函数。

$H_1(\ )$：由密码杂凑函数派生的密码函数。

hid：在本部分中，用一个字节表示的加密私钥生成函数识别符，由 KGC 选择并公开。

ID_A：用户 A 的标识，可以唯一确定用户 A 的公钥。

ID_B：用户 B 的标识，可以唯一确定用户 B 的公钥。

$KDF(\ )$：密钥派生函数。

N：循环群 G_1、G_2 和 G_T 的阶，为大于 2^{191} 的素数。

$P_{pub\text{-}e}$：加密主公钥。

P_1：群 G_1 的生成元。

P_2：群 G_2 的生成元。

r_A：密钥交换中用户 A 产生的临时密钥值。

r_B：密钥交换中用户 B 产生的临时密钥值。

SK_A，SK_B：密钥交换协议商定的共享秘密密钥。

ke：加密主私钥。

$\langle P\rangle$：由元素 P 生成的循环群。

$[u]P$：加法群 G_1、G_2 中元素 P 的 u 倍。

$\lceil x\rceil$：顶函数，不小于 x 的最小整数。例如，$\lceil 7\rceil=7$，$\lceil 8.3\rceil=9$。

$\lfloor x\rfloor$：底函数，不大于 x 的最大整数。例如，$\lfloor 7\rfloor=7$，$\lfloor 8.3\rfloor=8$。

$x\parallel y$：x 与 y 的拼接，x 和 y 是比特串或字节串。

$[x,y]$：不小于 x 且不大于 y 的整数的集合。

β：扭曲线参数。

5 算法参数与辅助函数

5.1 总则

本部分规定了一个用椭圆曲线对实现的基于标识的密钥交换协议。参与密钥交换的发起方用户 A 和响应方用户 B 各自持有一个标识和一个相应的加密私钥，加密私钥均由密钥生成中心通过加密主私钥和用户的标识结合产生。用户 A 和用户 B 通过交互的信息传递，用标识和各自的加密私钥来商定一个只有他们知道的秘密密钥，用户双方可以通过可选项实现密钥确认。这个共享的秘密密钥通常用在某个对称密码算法中。该密钥交换协议能够用于密钥管理和协商。

5.2 系统参数组

系统参数组包括曲线识别符 cid，椭圆曲线基域 F_q 的参数，椭圆曲线方程参数 a 和 b，扭曲线参数 β（若 cid 的低 4 位为 2），曲线阶的素因子 N 和相对于 N 的余因子 cf，曲线 $E(F_q)$ 相对于 N 的嵌入次数 k，$E(F_{q^{d_1}})$（d_1 整除 k）的 N 阶循环子群 G_1 的生成元 P_1，$E(F_{q^{d_2}})$（d_2 整除 k）的 N 阶循环子群 G_2 的生成元 P_2，双线性对 e 的识别符 eid，（选项）G_2 到 G_1 的同态映射 ψ。

双线性对 e 的值域为 N 阶乘法循环群 G_T。

系统参数的详细描述及其验证参见 GM/T 0044.1—2016 的第 7 章。

5.3 系统加密主密钥和用户加密密钥的产生

KGC 产生随机数 $ke\in[1,N-1]$ 作为加密主私钥，计算 G_1 中的元素 $P_{pub\text{-}e}=[ke]P_1$ 作为加密主公钥，则加密主密钥对为 $(ke,P_{pub\text{-}e})$。KGC 秘密保存 ke，公开 $P_{pub\text{-}e}$。

KGC 选择并公开用一个字节表示的加密私钥生成函数识别符 hid。

用户 A 和用户 B 的标识分别为 ID_A 和 ID_B。为产生用户 A 的加密私钥 de_A，KGC 首先在有限域 F_N 上计算 $t_1=H_1(ID_A\parallel hid,N)+ke$，若 $t_1=0$ 则需重新产生加密主私钥，计算和公开加密主公钥，并更新已有用户的加密私钥；否则计算 $t_2=ke\cdot t_1^{-1}$，然后计算 $de_A=[t_2]P_2$。为产生用户 B 的加密私钥 de_B，KGC 首先在有限域 F_N 上计算 $t_3=H_1(ID_B\parallel hid,N)+ke$，若 $t_3=0$ 则需重新产生加密主私钥，计算和公开加密主公钥，并更新已有用户的加密私钥；否则计算 $t_4=ke\cdot t_3^{-1}$，然后计算 $de_B=[t_4]P_2$。

5.4 辅助函数

5.4.1 概述

在本部分规定的基于标识的密钥交换协议中，涉及 3 类辅助函数：密码杂凑函数、密钥派生函数与

随机数发生器。这3类辅助函数的强弱直接影响密钥交换协议的安全性。

5.4.2 密码杂凑函数

5.4.2.1 密码杂凑函数 $H_v(\ )$

密码杂凑函数 $H_v(\ )$的输出是长度恰为 v 比特的杂凑值。本部分规定使用国家密码管理主管部门批准的密码杂凑函数，如SM3密码杂凑算法。

5.4.2.2 密码函数 $H_1(\ )$

密码函数 $H_1(Z,n)$的输入为比特串 Z 和整数 n，输出为一个整数 $h_1\in[1,n-1]$。$H_1(Z,n)$需要调用密码杂凑函数 $H_v(\ )$。关于密码杂凑函数 $H_v(\ )$，应符合5.4.2.1的规定。

密码函数 $H_1(Z,n)$：

输入：比特串 Z，整数 n。

输出：整数 $h_1\in[1,n-1]$。

步骤1：初始化一个32比特构成的计数器 $ct=0x00000001$；

步骤2：计算 $hlen=8\times\lceil(5\times(\log_2 n))/32\rceil$；

步骤3：对 i 从1到 $\lceil hlen/v\rceil$ 执行：

步骤3.1：计算 $Ha_i=H_v(0x01\ \|\ Z\ \|\ ct)$；

步骤3.2：$ct++$；

步骤4：若 $hlen/v$ 是整数，令 $Ha!_{\lceil hlen/v\rceil}=Ha_{\lceil hlen/v\rceil}$，

否则令 $Ha!_{\lceil hlen/v\rceil}$ 为 $Ha_{\lceil hlen/v\rceil}$ 最左边的 $(hlen-(v\times\lfloor hlen/v\rfloor))$ 比特；

步骤5：令 $Ha=Ha_1\ \|\ Ha_2\ \|\ \cdots\ \|\ Ha_{\lceil hlen/v\rceil-1}\ \|\ Ha!_{\lceil hlen/v\rceil}$，按GM/T 0044.1—2016的6.2.4和6.2.3给出的细节将 Ha 的数据类型转换为整数；

步骤6：计算 $h_1=(Ha\ \bmod\ (n-1))+1$。

5.4.2.3 密码函数 $H_2(\ )$

密码函数 $H_2(Z,n)$的输入为比特串 Z 和整数 n，输出为一个整数 $h_2\in[1,n-1]$。$H_2(Z,n)$需要调用密码杂凑函数 $H_v(\ )$。关于密码杂凑函数 $H_v(\ )$，应符合5.4.2.1的规定。

密码函数 $H_2(Z,n)$：

输入：比特串 Z，整数 n。

输出：整数 $h_2\in[1,n-1]$。

步骤1：初始化一个32比特构成的计数器 $ct=0x00000001$；

步骤2：计算 $hlen=8\times\lceil(5\times(\log_2 n))/32\rceil$；

步骤3：对 i 从1到 $\lceil hlen/v\rceil$ 执行：

步骤3.1：计算 $Ha_i=H_v(0x02\ \|\ Z\ \|\ ct)$；

步骤3.2：$ct++$；

步骤4：若 $hlen/v$ 是整数，令 $Ha!_{\lceil hlen/v\rceil}=Ha_{\lceil hlen/v\rceil}$，

否则令 $Ha!_{\lceil hlen/v\rceil}$ 为 $Ha_{\lceil hlen/v\rceil}$ 最左边的 $(hlen-(v\times\lfloor hlen/v\rfloor))$ 比特；

步骤5：令 $Ha=Ha_1\ \|\ Ha_2\ \|\ \cdots\ \|\ Ha_{\lceil hlen/v\rceil-1}\ \|\ Ha!_{\lceil hlen/v\rceil}$，按GM/T 0044.1—2016的6.2.4和6.2.3给出的细节将 Ha 的数据类型转换为整数；

步骤6：计算 $h_2=(Ha\ \bmod\ (n-1))+1$。

5.4.3 密钥派生函数

密钥派生函数的作用是从一个共享的秘密比特串中派生出密钥数据。在密钥协商过程中，密钥派

生函数作用在密钥交换所获共享的秘密比特串上，从中产生所需的会话密钥或进一步加密所需的密钥数据。

密钥派生函数需要调用密码杂凑函数。

设密码杂凑函数为 $H_v(\ )$，其输出是长度恰为 v 比特的杂凑值。

密钥派生函数 $KDF(Z,klen)$：

输入：比特串 Z（双方共享的数据），整数 $klen$（表示要获得的密钥数据的比特长度，要求该值小于 $(2^{32}-1)v$）。

输出：长度为 $klen$ 的密钥数据比特串 K。

步骤 1：初始化一个 32 比特构成的计数器 $ct=0$x00000001；

步骤 2：对 i 从 1 到 $\lceil klen/v \rceil$ 执行：

步骤 2.1：计算 $Ha_i=H_v(Z \| ct)$；

步骤 2.2：$ct++$；

步骤 3：若 $klen/v$ 是整数，令 $Ha!_{\lceil klen/v \rceil}=Ha_{\lceil klen/v \rceil}$，

否则令 $Ha!_{\lceil klen/v \rceil}$ 为 $Ha_{\lceil klen/v \rceil}$ 最左边的 $(klen-(v\times\lfloor klen/v \rfloor))$ 比特；

步骤 4：令 $K=Ha_1 \| Ha_2 \| \cdots \| Ha_{\lceil klen/v \rceil-1} \| Ha!_{\lceil klen/v \rceil}$。

5.4.4 随机数发生器

本部分规定使用国家密码管理主管部门批准的随机数发生器。

6 密钥交换协议及流程

6.1 密钥交换协议

设用户 A 和用户 B 协商获得密钥数据的长度为 $klen$ 比特，用户 A 为发起方，用户 B 为响应方。

用户 A 和用户 B 双方为了获得相同的密钥，应实现如下运算步骤：

用户 A：

A1：计算群 G_1 中的元素 $Q_B=[H_1(ID_B \| hid,N)]P_1+P_{pub\text{-}e}$；

A2：产生随机数 $r_A\in[1,N-1]$；

A3：计算群 G_1 中的元素 $R_A=[r_A]Q_B$；

A4：将 R_A 发送给用户 B；

用户 B：

B1：计算群 G_1 中的元素 $Q_A=[H_1(ID_A \| hid,N)]P_1+P_{pub\text{-}e}$；

B2：产生随机数 $r_B\in[1,N-1]$；

B3：计算群 G_1 中的元素 $R_B=[r_B]Q_A$；

B4：按 GM/T 0044.1—2016 的 4.5 给出的细节验证 $R_A\in G_1$ 是否成立，若不成立则协商失败；否则计算群 G_T 中的元素 $g_1=e(R_A,de_B)$，$g_2=e(P_{pub\text{-}e},P_2)^{r_B}$，$g_3=g_1^{r_B}$，按 GM/T 0044.1—2016 的 6.2.6 和 6.2.5 给出的细节将 g_1,g_2,g_3 的数据类型转换为比特串；

B5：按 GM/T 0044.1—2016 的 6.2.8 和 6.2.5 给出的细节把 R_A 和 R_B 的数据类型转换为比特串，计算 $SK_B=KDF(ID_A \| ID_B \| R_A \| R_B \| g_1 \| g_2 \| g_3,klen)$；

B6：（选项）计算 $S_B=Hash(0$x82 $\| g_1 \| Hash(g_2 \| g_3 \| ID_A \| ID_B \| R_A \| R_B))$；

B7：将 R_B、（选项 S_B）发送给用户 A；

用户 A：

A5：按 GM/T 0044.1—2016 的 4.5 给出的细节验证 $R_B\in G_1$ 是否成立，若不成立则协商失败；否则

计算群 G_T 中的元素 $g_1'=e(P_{pub\text{-}e},P_2)^{r_A}$，$g_2'=e(R_B,de_A)$，$g_3'=(g_2')^{r_A}$，按GM/T 0044.1—2016 的 6.2.6 和 6.2.5 给出的细节将 g_1'，g_2'，g_3' 的数据类型转换为比特串；

A6：按 GM/T 0044.1—2016 的 6.2.8 和 6.2.5 给出的细节把 R_A 和 R_B 的数据类型转换为比特串，(选项)计算 $S_1=Hash(0x82\|g_1'\|Hash(g_2'\|g_3'\|ID_A\|ID_B\|R_A\|R_B))$，并检验 $S_1=S_B$ 是否成立，若等式不成立则从 B 到 A 的密钥确认失败；

A7：计算 $SK_A=KDF(ID_A\|ID_B\|R_A\|R_B\|g_1'\|g_2'\|g_3',klen)$；

A8：(选项)计算 $S_A=Hash(0x83\|g_1'\|Hash(g_2'\|g_3'\|ID_A\|ID_B\|R_A\|R_B))$，并将 S_A 发送给用户 B。

用户 B：

B8：(选项)计算 $S_2=Hash(0x83\|g_1\|Hash(g_2\|g_3\|ID_A\|ID_B\|R_A\|R_B))$，并检验 $S_2=S_A$ 是否成立，若等式不成立则从 A 到 B 的密钥确认失败。

6.2 密钥交换协议流程

密钥交换协议流程如图 1。

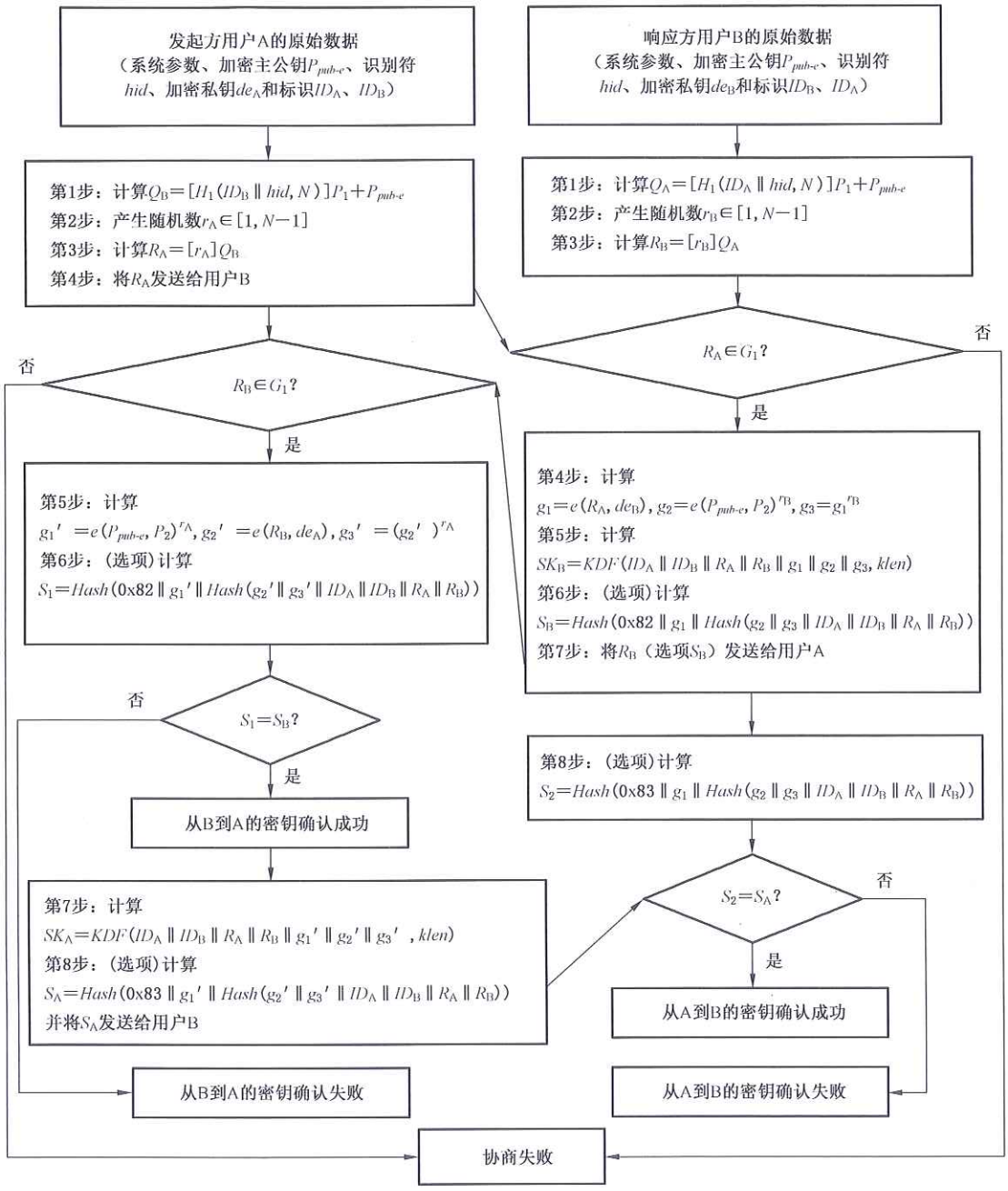
发起方用户A的原始数据
（系统参数、加密主公钥P_{pub-e}、识别符hid、加密私钥de_A和标识ID_A、ID_B）
响应方用户B的原始数据
（系统参数、加密主公钥P_{pub-e}、识别符hid、加密私钥de_B和标识ID_B、ID_A）
第1步：计算$Q_B=[H_1(ID_B \| hid, N)]P_1+P_{pub-e}$
第2步：产生随机数$r_A\in[1, N-1]$
第3步：计算$R_A=[r_A]Q_B$
第4步：将R_A发送给用户B
第1步：计算$Q_A=[H_1(ID_A \| hid, N)]P_1+P_{pub-e}$
第2步：产生随机数$r_B\in[1, N-1]$
第3步：计算$R_B=[r_B]Q_A$
$R_A\in G_1$?
否
是
$R_B\in G_1$?
否
是
第4步：计算
$g_1=e(R_A, de_B)$, $g_2=e(P_{pub-e}, P_2)^{r_B}$, $g_3=g_1^{r_B}$
第5步：计算
$SK_B=KDF(ID_A \| ID_B \| R_A \| R_B \| g_1 \| g_2 \| g_3, klen)$
第6步：（选项）计算
$S_B=Hash(0x82 \| g_1 \| Hash(g_2 \| g_3 \| ID_A \| ID_B \| R_A \| R_B))$
第7步：将R_B（选项S_B）发送给用户A
第5步：计算
$g_1'=e(P_{pub-e}, P_2)^{r_A}$, $g_2'=e(R_B, de_A)$, $g_3'=(g_2')^{r_A}$
第6步：（选项）计算
$S_1=Hash(0x82 \| g_1' \| Hash(g_2' \| g_3' \| ID_A \| ID_B \| R_A \| R_B))$
否
$S_1=S_B$?
是
第8步：（选项）计算
$S_2=Hash(0x83 \| g_1 \| Hash(g_2 \| g_3 \| ID_A \| ID_B \| R_A \| R_B))$
从B到A的密钥确认成功
第7步：计算
$SK_A=KDF(ID_A \| ID_B \| R_A \| R_B \| g_1' \| g_2' \| g_3', klen)$
第8步：（选项）计算
$S_A=Hash(0x83 \| g_1' \| Hash(g_2' \| g_3' \| ID_A \| ID_B \| R_A \| R_B))$
并将S_A发送给用户B
$S_2=S_A$?
否
是
从A到B的密钥确认成功
从B到A的密钥确认失败
从A到B的密钥确认失败
协商失败

图 1　密钥交换协议流程

中华人民共和国密码
行业标准
SM9 标识密码算法
第 3 部分：密钥交换协议
GM/T 0044.3—2016

*

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.net.cn
总编室：(010)68533533　发行中心：(010)51780238
读者服务部：(010)68523946

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230　1/16　印张 0.75　字数 18 千字
2016 年 12 月第一版　2016 年 12 月第一次印刷

*

书号：155066·2-30457　定价　16.00 元

GM/T 0044.3-2016