ICS 35.040
L 80

中华人民共和国国家标准

GB/T 34953.4—2020

信息技术　安全技术　匿名实体鉴别
第4部分:基于弱秘密的机制

Information technology—Security techniques—Anonymous entity authentication—Part 4: Mechanisms based on weak secrets

(ISO/IEC 20009-4:2017,MOD)

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

GB/T 34953《信息技术　安全技术　匿名实体鉴别》分为4个部分：

——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4部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分使用重新起草法修改采用ISO/IEC 20009-4:2017《信息技术　安全技术　匿名实体鉴别　第4部分：基于弱秘密的机制》。

本部分与ISO/IEC 20009-4:2017相比结构上有调整，调整6.3为6.2，其他条编号依次修改。

本部分与ISO/IEC 20009-4:2017的技术性差异及其原因如下：

——关于规范性引用文件，本部分做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第2章“规范性引用文件”中，具体调整如下：

- 用修改采用国际标准的GB/T 15852.2代替ISO/IEC 9797-2，并规定使用的杂凑算法应遵循相关国家标准和行业标准；
- 用等同采用国际标准的GB/T 34953.1代替ISO/IEC 29000-1；
- 用修改采用国际标准的GB/T 36624—2018代替ISO/IEC 19772:2009；
- 删除ISO/IEC 10118-3，ISO/IEC 10118-3规定了本部分机制使用的杂凑算法，并规定使用的杂凑算法应遵循相关国家标准和行业标准；
- 删除ISO/IEC 18033-4，ISO/IEC 18033-4规定了本部分机制使用的序列密码算法，并规定使用的序列密码算法应遵循相关国家标准和行业标准。

——增加了缩略语“MAC”和“PAEA”(见4.1)。

——删除了ISO/IEC 20009-4:2017中包含国际专利的6.2:SKI机制，以使本部分更好地适用于我国当前的应用环境(见ISO/IEC 20009-4:2017的6.2)。

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：中国科学院软件研究所、公安部第三研究所、北京数字认证股份有限公司、中国科学院数据与通信保护研究教育中心、中国电子技术标准化研究院。

本部分主要起草人：张振峰、张立武、张严、冯登国、杨明慧、刘丽敏、王惠莅、陈景燕、江伟玉、杨糠。

引　言

自从计算机问世以来，通过输入用户标识和口令的方式进行用户身份鉴别得到了广泛的应用并且一直是最为普遍的鉴别方式。每天都有数以亿计的口令鉴别在网络空间中发生。口令鉴别被广泛接纳的原因之一在于不需要额外的辅助设施并且用户只需要记住口令即可在任意时间任意地点进行身份鉴别的轻便性。ISO/IEC 11770-4:2016 描述了基于口令(口令通常是弱秘密)的密钥管理方案。这些方案可以被用来实现基于口令的实体鉴别。

同时，网络空间的个人隐私安全正受到被越来越多的关注。在网络空间中进行实体鉴别时对用户隐私进行保护是个人隐私保护的关键步骤。GB/T 34953 系列标准规范了实体鉴别隐私保护的技术，用于支持匿名实体鉴别。本部分关注基于弱秘密的匿名实体鉴别机制。特别是，本部分描述了基于口令的匿名实体鉴别(PAEA)机制，PAEA 能够为口令鉴别过程提供隐私保护。

PAEA 机制需要解决的主要问题是如果将口令等弱秘密直接应用于那些基于强秘密构造的匿名鉴别机制，则会因口令的弱秘密性质泄露秘密，导致用户隐私无法受到保护。本部分描述了两种 PAEA 机制：仅采用口令的 PAEA 和基于辅助存储设施的机制。在仅采用口令的 PAEA 机制中，用户在服务器注册并记住其用于鉴别的口令数据，然后与在非匿名口令鉴别机制中一样地使用其口令进行鉴别。在基于辅助存储设施的机制中，用户不仅要记住他们的口令，还要同时持有一个口令包裹，该口令包裹可以暴露给敌手但是不会危害用户的隐私安全。同时用户口令的验证信息将不储存于服务器中。上述两种机制在不同的应用场景下具有其各自的优势。

信息技术　安全技术　匿名实体鉴别
第4部分：基于弱秘密的机制

1　范围

GB/T 34953的本部分规定了基于弱秘密的匿名实体鉴别机制、每种机制的具体操作步骤以及详细的输入输出。

本部分适用于服务器在无法获取可用来识别用户具体身份信息的情况下对用户进行校验，确认其属于特定用户群组的场景。

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。

GB/T 15852.2　信息技术　安全技术　消息鉴别码　第2部分：采用专用杂凑函数的机制（GB/T 15852.2—2012，ISO/IEC 9797-2：2002，MOD）

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

GB/T 36624—2018　信息技术　安全技术　可鉴别的加密机制（ISO/IEC 19772：2009，MOD）

ISO/IEC 11770-4：2006　信息技术　安全技术　密钥管理　第4部分：基于弱秘密的机制（Information technology—Security techniques—Key management—Part 4：Mechanisms based on weak secrets）

3　术语和定义

GB/T 34953.1界定的以及下列术语和定义适用于本文件。

3.1

交换群　abelian group

满足对S中的所有元素 a 与 b，有 $a*b=b*a$ 的群（S，*）。

3.2

可鉴别的加密　authenticated encryption

使用密码学算法对数据进行的（可逆）操作，使得生成的密文不能被非授权实体在不被探测到的情况下修改，即：提供数据机密性、数据完整性与数据源鉴别。

3.3

鉴别凭证　authentication credential

包含可用来对实体进行鉴别的信息的凭证。

3.4

认证器　authenticator

作为鉴别机制的一部分被发送，并且被另一方验证的数据串。

3.5

声明方　claimant

在鉴别中，作为委托人或代表委托人的实体。

注：声明方包括代表委托人进行鉴别交互所需的功能及秘密数据。

3.6

抗碰撞杂凑函数　collision-resistant hash-function

满足下列性质的杂凑函数：找到映射到相同杂凑值的两个输入在计算上是不可行的。

注：计算不可行性依赖于特定的安全需求及环境。

3.7

凭证　credential

对一个身份的描述。通常用来帮助对其所描述的身份对应的身份信息进行鉴别，凭证所描述的身份信息可打印于纸质文件或储存于物理令牌中，以用来声明该信息的合法性。

示例：凭证可以是用户名、用户名与口令的组合、个人识别码(PIN)、智能卡、令牌、指纹、护照等。

3.8

循环群　cyclic group

满足以下性质的交换群(G，*)：存在 G 中的元素 g，对于每个 G 中的每个元素 a，都存在整数 i 使得 $a=g^i$，g 称为 G 的生成元。

3.9

可区分标识符　distinguishing identifier

可无二义性区分某个实体的信息。

3.10

穷举搜索　exhaustive search

对秘密值的所有可能取值进行遍历的攻击方法。

注：穷举搜索也被称为暴力破解。

3.11

域　field

满足以下条件的集合 S 与定义在其上的对运算(+，*)：a)对 S 中的任意元素 a,b,c，有 $a*(b+c)=a*b+a*c$；b)S 与+操作构成一个单位元为 0 的**交换群**(3.1)；c)S 中除 0 元素以外的元素与 * 操作构成一个交换群。

3.12

有限域　finite field

包含有限个元素的域。

注：对于任意的正整数 m 和素数 p，均存在包含正好 p^m 个元素的有限域。该有限域是同构唯一的，记为 $F(p^m)$，其中 p 称为 $F(p^m)$ 的特征。

3.13

群　group

满足以下条件的集合 S 与定义在其上的运算 *：a)对 S 中的任意元素 a,b,c，有 $a*(b*c)=(a*b)*c$；b)S 中存在单位元 e，对 S 中的任意元素 a，有 $a*e=e*a=a$；c)对 S 中的任意元素 a，存在逆元素 a^{-1} 满足 $a*a^{-1}=a^{-1}*a=e$。

3.14

群生成元　group generator

循环群的生成元。

3.15

同态加密　homomorphic encryption

一种允许第三方在密文状态下对明文进行操作的对称或非对称加密。

注：第三方指除加密方与解密方以外的任何实体。

3.16

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

在密钥的作用下将比特串映射到固定长度位比特的计算函数，满足如下两个性质：

——对于任意的密钥和任意的输入串，该函数可被有效计算；

——对于任何固定的密钥，在不给定有关该密钥的先验知识的条件下，对于任意新的输入串，即使给定了若干输入串的集合及其对应的输出，且该集合中第 i 个输入的值可基于对前 $i-1$ 个输入值进行观察后再选择，计算该函数的输出仍是计算不可行的。

注 1：MAC 算法有时也被称为密码校验函数。

注 2：计算不可行性依赖于特定的安全需求及环境。

3.17

离线穷举搜索　offline exhaustive search

在不与任何授权方进行交互的情况下执行的穷举搜索。

3.18

口令　password

可被记忆的用来进行实体鉴别的私密单词、词组、数字或者字母序列。

3.19

口令验证数据　password verification data

用于检验实体是否掌握某个特定口令知识的数据。

3.20

口令包裹凭证　password wrapped credential

由口令产生的，能够抵抗离线穷举搜索攻击的鉴别凭证。

3.21

素域　prime field

包含素数个元素的有限域。

3.22

假名　pseudo distinguishing identifier

只在一段时间内有效的能够明确区分某个实体的信息。

3.23

安全素数　secure prime

满足 $(p-1)/2$ 仅包含大素数因子的奇素数 p。

3.24

系统参数　system parameters

对加密方案或者函数的选择。

4　符号、缩略语和转化原语

4.1　符号和缩略语

GB/T 34953.1 界定的以及下列符号和缩略语适用于本文件。

AD_K：使用 K 作为密钥的可鉴别的加密机制的解密函数，应选择 GB/T 36624—2018 中规定的

机制。

AE_K：使用 K 作为密钥的可鉴别的加密机制的加密函数，应选择 GB/T 36624—2018 中规定的机制。

$a \bmod n$：使 $r \equiv a(\bmod n)$ 且 $r \in [0, n-1]$ 成立的唯一整数 r，其中 a 为整数，n 为正整数。

$a \equiv b(\bmod n)$：整数 a 和 b 间的关系，当且仅当 a 和 b 对 n 同余（即 $n \mid (a-b)$）时成立，其中 n 为非零整数。

$a^{-1} \bmod n$：使 $b \in [1, n-1]$ 且 $ab \equiv 1(\bmod n)$ 成立的唯一整数 b，其中 a 是整数，n 是正整数，$\gcd(a, n) = 1$。

CRL：凭证撤销列表(Credential Revocation List)。

DEC_{pw}：符合密码相关国家标准和行业标准的序列密码算法的解密函数，使用口令 pw（和随机的初始值，如算法需要）派生的密钥作为密钥。

ENC_{pw}：符合密码相关国家标准和行业标准的序列密码算法的加密函数，使用口令 pw（和随机的初始值，如算法需要）派生的密钥作为密钥。

$E(F(p))$：椭圆曲线上值为 $F(p)$ 的点以及一个额外的无穷远点 O_E 构成的集合（关于该集合的详细定义可参见 ISO/IEC 15946-1）。

$F(p)$：一个包含了 p 个元素的有限域，其中 p 是素数或者素数的幂。

$\gcd(a, b)$：a 和 b 的最大公约数，其中 a，b 为整数。即能同时整除 a 和 b 的最大的正整数（若 $a = 0$ 或 $b = 0$，则为 0）。

g^x：如果 g 是有限域 $F(p)$ 的元素，本符号表示在有限域中计算的 g^x，其中 g 是阶为素数 q 的循环群上的生成元。如果 g 是椭圆曲线上的点，则表示椭圆曲线标量乘法 $[x]g$，其中 x 表示标量，g 表示椭圆曲线上素数阶 q 的一个基点。

$g_1 * g_2$：如果 g_1 和 g_2 是有限域 $F(p)$ 的元素，本符号表示在有限域中计算的 $g_1 * g_2$。如果 g_1 和 g_2 是椭圆曲线上的点，则表示定义在椭圆曲线的循环群操作符 + 上的 $g_1 + g_2$。

g_1 / g_2：如果 g_1 和 g_2 是有限域 $F(p)$ 的元素，本符号表示在有限域中计算的 g_1 / g_2。如果 g_1 和 g_2 是椭圆曲线上的点，则表示定义在椭圆曲线的循环群操作符 − 上的 $g_1 - g_2$。

H：一个抗碰撞杂凑函数，以一个比特/字节串作为输入并输出一个比特/字节串，应使用符合密码相关国家标准和行业标准的杂凑函数机制。

HD_{sk}：使用私钥 sk 的同态加密机制的解密函数。

HE_{pk}：使用公钥 pk 的同态加密机制的加密函数。

H_g：一个抗碰撞的杂凑函数，以一个比特/字节串作为输入并输出一个以素数 q 为阶的循环群的生成元，应使用符合密码相关国家标准和行业标准的抗碰撞杂凑函数机制与 ISO/IEC 11770-4:2006 中规定的 R_{1DL} 或 R_{1EC} 函数（将比特串转化为循环群元素）的组合。

H_λ：一个抗碰撞的杂凑函数，以一个比特/字节串作为输入并输出一个长度为 λ 的比特/字节串，应使用符合密码相关国家标准和行业标准的杂凑函数机制并将其截断为 λ 位。

I_S：以字节串形式表示的鉴别服务器 S 的可区分标识符。

I_U：以字节串形式表示的可区分标识符，代表一个用户 U、一个声明方或一个群组的用户。

I_{U_i}：以字节串形式表示的可区分标识符，代表用户群组 $U_1, U_2, \cdots, U_n$ 中的一个用户 U_i。

$\underline{I}_{U_i}$：以字节串形式表示的用户 U_i 的假名。

$MAC_\lambda(MK, MESSAGE)$：一个 MAC 算法，以一个比特/字节串 MK 作为 MAC 生成密钥，并以一个待鉴别的比特/字节串 MESSAGE 作为输入，输出一个长度为 λ 的比特/字节串。

$Ocheck$：检验给定群组元素的阶是否为素数 q 或更高的函数，该函数取决于待检验的群元素的类型。a) 对于素数域 $F(p)$ 中的群组元素并且 p 是安全素数的情况，它以 $F(p)$ 中的元素 b 为输入，若 b 不为 $-1, 0, 1(\bmod p)$ 则输出合法，否则输出非法；b) 对于素数域 $F(p)$ 中的群组元素并且 p 不是安全

素数的情况，它以 $F(p)$ 中的元素 b 为输入，若 b 不为 $-1,0,1(\mathrm{mod}p)$ 且 $b^q \equiv 1(\mathrm{mod}p)$ 则输出合法，否则输出非法；c) 对于一个椭圆曲线 $E(F(p))$ 上的点来说，它以 $F(p)\times F(p)$ 中的元素 b 作为输入，并且当 $b^{\#E/q}$ 和无穷远点 O_E 不相等输出合法，否则输出不合法。

O_E：椭圆曲线中的无穷远点。

PWF：口令文件。

$params$：系统公开参数。

pvd_U：与用户 U 相关联的口令验证数据。

pw_U：与用户 U 相关联的口令。

$ServK$：由鉴别服务器秘密保管的服务器密钥。

SK：会话密钥。

$secparam$：安全参数，即代表某机制实例的安全位数长度的参数可行的。

注：通常的选择为 128 或更高。

$\tilde{x} \| \tilde{y}$：如果 $\tilde{x}$ 和 $\tilde{y}$ 表示比特/字节串，则表示将 y 拼接到 x 之后得到的连接字符串。

$|x|$：数字 x 的比特长度。

λ_k：对称密钥 k 的比特长度。

$\lambda_{\underline{U}}$：假名 $\underline{I}_U$ 的比特长度。

λ_v：以 V_U, V'_U, V_S, V'_S 表示的认证器的比特长度。

$\#E$：椭圆曲线 $E(F(p))$ 上的有理数点的个数，包括无穷点 O_E（参见 ISO/IEC 15946-1）。

$[i,j]$：由满足 $i \leqslant m \leqslant j$ 的全部整数 m 构成的集合。

$< x_1,\cdots,x_l >$：由元素 $x_1,\cdots,x_l$ 组成的 l-元组。

$\perp$：空。

MAC：消息鉴别码（Message Authentication Code）

PAEA：基于口令的匿名实体鉴别（Password-based Anonymous Entity Authentication）

4.2 转化原语

EC2OSP——从椭圆曲线到字节串的转化原语，具体实现参见 ISO/IEC JTC 1/SC 27/ WG 2 Standing Document 7 中的转化函数 EC2OS(,compressed)（该函数的第一个参数即本转化原语的输入，第二个参数使用 compressed）。

FE2OSP——从域元素到字节串的转化原语，参见 ISO/IEC JTC 1/SC 27/WG 2 Standing Document 7。

GE2OSP——从循环群元素到字节串的转化原语。在有限域中，该原语的实现即 FE2OSP。在椭圆曲线中，该原语的实现即 EC2OSP。

5 基于口令的匿名实体鉴别的通用模型

5.1 参与者

基于口令的匿名实体鉴别机制的参与者包括鉴别服务器和从属于特定用户群组的用户。

注：用户群组中的用户可以是能够获得某种服务的用户或者是具有某种属性的用户，例如年龄大于 18 岁、男性、女性等。

5.2 PAEA 机制的种类

本部分定义了两种 PAEA 机制：仅采用口令和基于辅助存储设施的机制。在仅采用口令的 PAEA 机制中，每个用户在鉴别服务器中注册一个口令，服务器保存该口令对应的口令验证数据；对于鉴别而

言，口令是用户唯一需要的长期秘密，相应地，口令验证数据是服务器唯一需要的长期秘密。在基于辅助存储设施的 PAEA 机制中，每个用户在鉴别服务器注册口令，作为结果，用户获得一个口令包裹凭证，但是服务器并不保存口令验证数据。用户需要一个存储设备来管理口令包裹凭证，但存储设备本身不需要进一步的保护(即口令包裹凭证可放置于公开目录中)。在进行鉴别时，用户首先需要使用口令从口令包裹凭证中恢复出鉴别凭证，之后使用恢复出的鉴别凭证在不透露其身份的情况下向服务器证明其是特定用户群组中的一员。

5.3 仅采用口令的 PAEA 的构成

一个仅采用口令的 PAEA 机制由以下操作组成：

——**建立**：给定一个安全参数 $secparam$，产生元组 $<params, PWF=\perp>$，其中 $params$ 表示系统公开参数，PWF 表示一个初始化为空的私有口令文件。PWF 文件包含若干有序 2 元组 $<I_U, pvd_U>$，其中 I_U 表示用户 U 的可区分标识符，pvd_U 表示 U 的口令验证数据。每一个 2 元组对应群组中的一个成员。$params$ 将作为机制中其他操作的共通输入，为了简单起见，本部分将在后续输入描述中省略 $params$。

——**用户注册**：给定用户的可区分标识符 I_U 和口令 pw_U，以及来自服务器的口令文件 PWF。产生口令验证数据 pvd_U，然后将 $<I_U, pvd_U>$ 加入到 PWF 文件中。

——**匿名鉴别**：该操作是在用户和鉴别服务器之间执行的交互鉴别过程。给定和用户 U 关联的口令 pw_U 以及来自服务器的口令文件 PWF，两个实体互相进行身份鉴别(并且可选地协商出共通的会话密钥)。其中用户的身份鉴别为匿名地进行，即：服务器只能验证用户属于某个特定的用户群组，但是不能获取到任何可以在后续过程中识别用户具体身份的信息。当且仅当鉴别双方都输出 ACCEPT 时，匿名鉴别操作输出 ACCEPT (并可选地输出会话密钥)，否则，输出 REJECT。

——**用户撤销**：给定用户身份 I_U，与口令文件 PWF，从 PWF 中移除 $<I_U, pvd_U>$，并对需要重新计算的预计算数值进行更新。

注 1：对于任何仅采用口令的 PAEA 机制来说一个最基本的需求是正确性。即对于任意的 $<I_U, pvd_U>$，当且仅当其属于 PWF 时，鉴别操作接受 U。

注 2：匿名鉴别操作的描述中包括了双方的相互鉴别以及密钥交换。但是根据实际应用的需求，可以将鉴别操作限定为只进行单向鉴别，比如用户单纯地鉴别服务器身份或者服务器单纯地鉴别用户从属于某一特定用户群组，而不进行反向鉴别以及密钥交换。

5.4 基于辅助存储的 PAEA 的构成

一个基于辅助存储的 PAEA 机制由以下操作组成：

——**建立**：给定安全参数 $secparam$，产生元组 $<params, ServK>$，其中 $params$ 表示公开的系统参数，$ServK$ 表示由服务器秘密保存的服务器密钥。$params$ 将作为机制中其他操作的共通输入，为了简单起见，本部分将在后续输入描述中省略 $params$。

——**用户注册**：给定用户的可区分标识符 I_U、口令 pw_U 以及服务器的密钥 $ServK$，输出一个口令包裹凭证 $cred_{pw_U}$。$cred_{pw_U}$ 可以存储在任何用户可以访问到的地方，如：用户存储设备或者公开目录中。

——**匿名鉴别**：该操作是在用户和鉴别服务器之间执行的交互鉴别过程。给定口令包裹凭证 $cred_{pw_U}$、口令 pw_U 以及服务器的 $ServK$，输出一个口令包裹凭证 $cred_{pw_U}$，两个实体互相进行身份鉴别(并且可选地协商出共通的会话密钥)。其中用户的身份鉴别为匿名地进行，即：服务器只能验证用户属于某个特定的用户群体但是不能获取到任何可以在后续过程中识别用户具体身份的信息。当且仅当鉴别双方都输出 ACCEPT 时，匿名鉴别操作输出 ACCEPT (并可

选地输出会话密钥)，否则，输出 REJECT 。

——**用户撤销**：给定一个用户的可区分的标识符 I_U 以及口令包裹凭证 $cred_{pw_U}$ ，撤销 I_U 的鉴别凭证，并且更新 CRL（凭证撤销列表）以满足 $CRL_{new}=CRL_{old}\cup\{cred\}$ ，其中 CRL_{new} 表示更新后的 CRL ，CRL_{old} 表示未经更新的 CRL ，$cred$ 为 $cred_{pw_U}$ 中包含的原始凭证。CRL 是 $params$ 的一部分并且初始化为空。

注 1：对于任何基于辅助存储的 PAEA 机制来说一个最基本的需求是正确性。即对于任意和同一用户相关联的元组 $<pw_U,cred_{pw_U}>$ 而言，当且仅当 $cred\notin CRL$ 时，鉴别操作接受该用户。

注 2：匿名鉴别操作的描述中包括了双方的相互鉴别以及密钥交换。但是根据实际应用的需求，可以将鉴别操作限定为只进行单向鉴别，比如用户单纯地鉴别服务器身份或者服务器单纯地鉴别用户从属于某一特定用户群组，而不进行反向鉴别以及密钥交换。

5.5 PAEA 操作

鉴别服务器执行**建立**操作，服务器产生系统参数，若是基于辅助存储设施的 PAEA 机制，则服务器还需产生一个服务器密钥。服务器将系统参数公开发布，而服务器密钥则由服务器私密保存。

当一个用户在系统中登记时，用户通过执行**用户注册**操作在服务器中注册其口令。在仅采用口令的 PAEA 机制中，服务器需基于用户口令产生并保存口令验证数据。反之，在基于辅助存储设施的 PAEA 机制中服务器不为自己产生任何数据，但是会为用户颁发一个口令包裹凭证，该口令包裹凭证由用户口令保护的鉴别凭证产生。

用户和服务器通过执行**匿名鉴别**操作进行相互鉴别与密钥交换。

服务器可通过执行**用户撤销**操作撤销用户鉴别权限，在基于辅助存储设施的 PAEA 机制中表现为撤销用户的鉴别凭证。

6 仅采用口令的 PAEA 机制

6.1 概述

本章描述了一种仅采用口令的 PAEA 机制。本章中描述的 PAEA 机制的对象标识符定义见附录 A。

注：YZ 机制基于参考文献[5]，参考文献[5]中同时给出了相关的安全分析。

6.2 YZ 机制

6.2.1 建立

给定安全参数 $secparam$ ，本操作将创建或确立以下公开的系统参数：

a) 一个阶为 q 的素数阶循环群 G ，生成元为 g ，应满足：

   1) q 的比特位数至少是 $secparam$ 值的两倍；

   2) G 的选取应使得在其上的离散对数问题的困难度（以比特度量）难于或者等于 $secparam$ ；

   3) 当 g 是有限域 $F(p)$ 中的元素时，p 作为安全素数应满足：$(p-1)/q=2q_1q_2\cdots q_t$ ，其中 $q_i>q(1\leqslant i\leqslant t)$（见 ISO/IEC 11770-4:2006 中第 5 章），以减少当 p 不满足安全参数要求时，为了检验从对端接受到的群元素的阶或者在匿名鉴别操作中检验该元素的阶而产生的额外计算开销；

   4) 当 g 是一个椭圆曲线 $E(F(p))$ 中的椭圆曲线点时，$E(F(p))$ 的辅因子，即：$\#E/q$ 宜为 1（或当 1 不可行时为 2），以减少为了检验从对端接受到的群元素的阶而产生的额外计算开销。

b) 如 4.1 所定义的阶检验函数 $Ocheck()$ 、消息鉴别码算法 MAC_k(MK,MESSAGE) 、抗碰撞杂

凑函数 $H_1()$ 和 $H_g()$、可鉴别的加密算法的加解密操作 $AE_K()$ 和 $AD_K()$。

注：ISO/IEC 15946-1 包含了在椭圆曲线中生成循环群以及其生成元的推荐操作，使得在大多数情况下，素数域之上的椭圆曲线 $\#E/q$ 为 1，在二元扩展域上的 $\#E/q$ 为 2。

6.2.2 用户注册

用户注册流程描述如下：

a) 用户 U_i 或者服务器 S 产生用户的口令验证数据 $pvd_{U_i}=H_g(I_{U_i} \| pw_i)$，其中 I_{U_i} 为用户的可区分的标识符，pw_i 为对应的口令；

b) 服务器 S 将元组 $< I_{U_i}, pvd_{U_i} >$ 加入到服务器口令文件 PWF 中；

c) 将 U_i 加入到合法用户群组 U 中；

d) 用户 U_i 获取到 6.2.1 中选取的公开参数的可信副本。

注：U_i 可以被加入到任意数量的用户群组中。

6.2.3 匿名鉴别

在本操作中，用户鉴别服务器身份，并且服务器对一个预先定义好的用户群组中的用户身份进行鉴别同时保持该用户身份的匿名性。

匿名鉴别的操作描述如下：

——步骤 1：根据用户 U_i 的请求，服务器 S 初始化协议：

a) 从 Z_q^* 中随机选择数字 r_S。

b) 对 U 中的每个用户 $U_j(1 \leqslant j \leqslant n)$，计算 $A_j = pvd_{U_j}{}^{r_S}$。

c) 将 $< I_S, \{A_j\}_{1 \leqslant j \leqslant n} >$ 发送给用户 U_i。

——步骤 2：收到服务器 S 发送的消息 $< I_S, \{A_j\}_{1 \leqslant j \leqslant n} >$ 后，用户 U_i 执行以下操作：

a) 检验 $\{A_j\}_{1 \leqslant j \leqslant n}$ 中的数据彼此间不同并且对全部的 A_j，$\{OCheck(A_j)\}_{1 \leqslant j \leqslant n}$ 合法。如果任一检验不通过，则终止协议并输出 REJECT。

b) 选取与用户 U_i 相对应的 $\{A_j\}_{1 \leqslant j \leqslant n}$ 中的第 i 项。

c) 从 Z_q^* 中选取两个随机数 r_c、x，并计算 $X = g^x$，$T = A_i{}^{r_C}$，$X^* = T \cdot X$，$B = pvd_{U_j}{}^{r_C}$。

d) 将 $< X^*, B >$ 发送给服务器。

——步骤 3：当收到 $< X^*, B >$ 消息后，服务器 S 执行以下操作：

a) 如果 $OCheck(X^*)$ 或 $OCheck(B)$ 检验不合法，则终止并输出 REJECT。

b) 使用随机数 r_S 计算 $T' = B^{r_S}$ 并恢复 $X' = X''/T'$。

c) 从 Z_q^* 中选择随机数 y，并计算 $Y = g^y$ 和 $K' = (X')^y$。

d) 如果 $OCheck(K')$ 不合法，则终止并输出 REJECT。

e) 设置 $Trans = I_S \| \{GE2OSP(A_j)\}_{1 \leqslant j \leqslant n} \| GE2OSP(X'') \| GE2OSP(B) \| GE2OSP(Y)$ 以及 MAC 密钥 $MK = H(GE2OSP(K'))$。

f) 产生认证器 $V_S = MAC_{\lambda_v}(MK, 1 \| Trans \| GE2OSP(T'))$。

g) 将 $< Y, V_S >$ 发送给用户。

——步骤 4：当用户收到消息 $< Y, V_S >$ 后，执行以下操作：

a) 如果 $OCheck(Y)$ 或 $OCheck(V_S)$ 不合法，则终止并输出 REJECT。

b) 计算 $K = Y^x$。

c) 设置 $Trans = S \| \{GE2OSP(A_j)\}_{1 \leqslant j \leqslant n} \| GE2OSP(X^*) \| GE2OSP(B) \| GE2OSP(Y)$ 以及 MAC 密钥 $MK' = H(GE2OSP(K))$。

d) 检查 $V_S = MAC_{\lambda_v}(MK', 1 \| Trans \| GE2OSP(T))$ 是否成立，若不成立则终止协议并输出 REJECT。

e) 否则输出 ACCEPT[可选地输出会话密钥 $SK = MAC_{\lambda_k}(MK', 0 \| Trans \| GE2OSP(T'))$]。

f) 产生认证器 $V_U = MAC_{\lambda_v}(MK', 2 \| Trans \| GE2OSP(T'))$，并发送给服务器。

——步骤 5：当服务器收到消息 $< V_U >$，执行以下操作：

a) 检验 $V_U = MAC_{\lambda_v}(MK, 2 \| Trans \| GE2OSP(T))$ 是否成立。如果不成立则终止协议并输出 REJECT 。

b) 否则输出 ACCEPT[可选地输出会话密钥 $SK = MAC_{\lambda_k}(MK, 0 \| Trans \| GE2OSP(T))$]。

6.2.4 用户撤销

服务器 S 通过执行以下操作对用户 U_i 进行用户撤销：

a) 输入一个 $U_j (1 \leqslant j \leqslant n)$ 中的可区分标识符 I_{U_i} ；

b) 输入服务器私密保管的口令文件 PWF ；

c) 在 PWF 中查找条目 $< I_{U_i}, pvd_{U_i} >$ 并删除，即：$PWF_{new} = PWF_{old} - \{< I_{U_i}, pvd_{U_i} >\}$ 。

7 基于辅助存储设施的 PAEA 机制

7.1 概述

本章描述了一种基于辅助存储设施的 PAEA 机制——YZW 机制[6]。本章中描述的 PAEA 机制的对象标识符定义见附录 A。

7.2 YZW 机制

7.2.1 概述

给定安全参数 $secparam$ ，该机制需要以下算法：

a) 同态加密：

在第 7 章中描述的机制需要乘法同态加密，$HE_{pk}(\cdot)$ 与 $HD_{sk}(\cdot)$ 分别表示以 pk 为公钥的加密函数和以 sk 为私钥的解密函数。乘法同态加密满足 $HE_{pk}(m_1) \cdot HE_{pk}(m_2) = HE_{pk}(m_1 \cdot m_2)$，其中 $\cdot$ 表示乘法操作。ElGamal 加密机制即满足所需的乘法同态加密性质，ElGamal 加密机制的规范如下：

令 $(pk = g'^z, sk = z)$ 为公/私钥对，其中 $g' \in Z_q$，$z \in Z_{q'}^*$ ，q, q' 为满足 $q = 2q' + 1$ 的素数。

对于消息 $m \in Z_q$ ，加密实例 $HE_{pk}(m)$ 操作如下：

1) 选择随机数 $r \in Z_{q'}^*$ ，计算 $c_1 = g'^r (\mathrm{mod} q)$，$c_2 = m \cdot pk^r = m \cdot g'^{zr} (\mathrm{mod} q)$ ；

2) 令密文 $C = (c_1, c_2)$ 。

与之对应的解密实例 $HD_{sk}(C)$ 操作如下：

3) 计算 $m = c_2 / c_1^z$ 。

进一步考虑两个密文 $C_1 = (g'^{r_1}, m_1 \cdot pk'^{r_1})$，$C_2 = (g'^{r_2}, m_2 \cdot pk'^{r_2})$ ，则 C_1 与 C_2 的乘积 $C' = (g'^{r_1+r_2}, m_1 \cdot m_2 \cdot pk'^{r_1+r_2})$ ，显然 C' 是与明文 $m_1 \cdot m_2$ 相对应的密文。

b) 符合 GB/T 15852.2 要求的 MAC 算法，其中的杂凑函数应使用密码相关国家标准和行业标准的抗碰撞杂凑函数：

—— $MAC_{\lambda_v}: \{0,1\}^t \times \{0,1\}^* \rightarrow \{0,1\}^{\lambda_v}$ 。

c) 符合密码相关国家标准和行业标准要求的序列密码算法：

——$ENC_{pw}(\cdot) / DEC_{pw}(\cdot)$ 分别表示使用由口令 pw 派生(即：通过使用口令 pw 与抗碰撞的杂凑函数并取适当长度的输出)得到的密钥的加密/解密函数。

d) 符合密码相关国家标准和行业标准要求的抗碰撞杂凑函数：

—— $H_\lambda: \{0,1\}^* \rightarrow \{0,1\}^\lambda$ 。

7.2.2 建立

本操作生成公开的系统参数以及秘密的服务器密钥，由以下步骤组成：

a) 建立由群 G_1, G_2, G_3 组成的基群集以及一个双线性映射 $e: G_1 \times G_2 \rightarrow G_3$，其中 G_1, G_2, G_3 为阶是素数 q 的循环群。且 $|q|$ 应至少为 *secureparam* 的两倍。带双线性映射的 MNT 椭圆曲线满足 e 的要求。

b) 选择随机生成元 $a, b, d, g, g_0, g_1 \in G_1$ 以及 $h \in G_2$。选择随机数 $x \in Z_q^*$，并且计算 $W = h^x$。

c) 为乘法同态加密方案产生公/私钥对 (pk, sk)，$HE_{pk}(\cdot)/HD_{sk}(\cdot)$ 分别表示加密/解密操作。注意该乘法同态加密方案的明文空间应为 $\{0,1\}^l$，其中 $l \geqslant |q|$ 为满足 *secparam* 安全要求的大整数，且 $Z_q \subset \{0,1\}^l$。

d) 选择一个抗碰撞的杂凑函数 $H_\lambda: \{0,1\}^* \rightarrow \{0,1\}^\lambda$ 以及一个 MAC 算法 $MAC_{\lambda_v}: \{0,1\}^l \times \{0,1\}^* \rightarrow \{0,1\}^{\lambda_v}$。$\lambda$ 与 λ_v 应至少为 *secparam* 的两倍。

e) 设置系统的公开参数 $params = < q, G_1, G_2, G_3, e, a, b, d, g, g_0, g_1, h, W, pk, H_\lambda, MAC_{\lambda_v} >$ 以及秘密的服务器密钥 $servK = < x, sk >$。

注：ISO/IEC 15946-1 给出了生成循环群、群生成元以及双线性映射的推荐操作。

推荐应用建立一种定期更新系统参数的方法。在这种情况下，所有用户需要在服务器处重新进行注册并更新其凭证。本部分不规定这一流程的具体实现。

7.2.3 用户注册

在用户注册操作中，用户将在服务器进行注册以便使后者能够为前者颁发鉴别凭证。最后，用户将提交口令 pw，并且服务器使用服务器密钥颁发凭证。算法执行如下。

输入：

——系统参数 $params$；

——服务器密钥 $servK = < x, sk >$；

——用户标识符 I_U 和口令 pw。

输出：

——口令包裹凭证 $cred_{pw}$。

操作，按以下步骤计算 $cred_{pw}$：

a) 选择随机数 $k, s \in Z_q^*$，$m' \in [0, 2^l - 1]$，其中 l 为 $ENC_{pw}()$ 密钥流的位长度，且 $2^l - 1$ 远大于 q，然后计算 $m = m'(\mathrm{mod} q)$，$M = (a^m b^s d)^{1/(k+x)}$；

b) 使用通过 pw 生成的密钥对 M 进行序列密码加密，记为 $ENC_{pw}(m')$；

c) 使用 pk 为密钥对 s 进行同态加密，记为 $HE_{pk}(s)$；

d) 设置 $cred_{pw} = < M, ENC_{pw}(m'), k, HE_{pk}(s) >$；

e) 用户获取 7.2.1 中选取的公开的系统参数的可信副本。

注 1：在本算法中，隐含了该机制能够使服务器鉴别注册用户的真实性的事实。例如，用户向服务器出示用户的 IC，鉴别的细节是必须的，但是不在 7.2 的讨论范围之内。

注 2：给定 $< M, m, k, s >$，用户显然能够自己产生口令包裹凭证。因此，上述操作的一个代替方案是用户仅仅输入用户的标识符 I_U，从服务器获取到 $< M, m, k, s >$ 后，用户自己产生 $cred_{pw}$。

7.2.4 匿名鉴别

匿名鉴别操作能够使得服务器和用户互相鉴别，并(可选地)建立一个共同的会话密钥。

输入：

——系统参数 $params$；

——服务器密钥 $servK = < x, sk >$；

——口令包裹凭证 $cred_{pw} = < elem_1, elem_2, elem_3, elem_4 > = < M, ENC_{pw}(m'), k, HE_{pk}(s) >$ 以及用户口令 pw。

输出：

—— ACCEPT（可选地输出会话密钥 SK）或者 REJECT。

匿名鉴别操作由以下步骤组成：

——步骤 1：用户执行以下步骤以初始化协议：

a) 计算 $m' = DEC_{pw}(elem_2)$，$m = m'(\mathrm{mod}q)$，其中 $DEC_{pw}(\cdot)$ 为 $ENC_{pw}(\cdot)$ 的逆函数。

b) 选择随机数 $r \in Z_q^*$ 并计算 $s^* = HE_{pk}(r) \cdot elem_4 = HE_{pk}(r \cdot s)$。

c) 选择随机数 $x_1 \in Z_q^*$ 并计算 $X = g^{x_1}$。

d) 选择随机数 $N_U \in \{0,1\}^l$ 并计算 $N_U{}^* = HE_{pk}(N_U)$。

e) 按如下步骤计算 $< T_1, T_2, R_1, R_2 >$：

1) 计算 $\gamma = r^{-1}(\mathrm{mod}q)$；

2) 计算 $B_e = (e(M, W \cdot h^k) / (e(a,h))^m \cdot e(d,h)))^r$；

3) 选择随机数 $\alpha, \mu \in Z_q^*$；

4) 计算 $T_1 = M \cdot g_0{}^\alpha$ 和 $T_2 = g_1{}^\alpha \cdot g_0{}^\mu$；

5) 选择随机数 $r_m, r_k, r_\gamma, r_\alpha, r_\beta, r_\mu \in Z_q^*$；

6) 计算 $R_1 = e(T_1,h)^{-r_k} \cdot e(a,h)^{r_m} \cdot B_e{}^{r_\gamma} \cdot e(g_0,W)^{r_\alpha} \cdot e(g_0,h)^{r_\beta}$ 和 $R_2 = g_1{}^{r_\alpha} \cdot g_0{}^{r_\mu}$。

f) 发送 $< s^*, X, N_U{}^*, < T_1, T_2, R_1, R_2 >>$ 到服务器以初始化协议。

——步骤 2：当收到用户发来的消息 $< s^*, X, N_U{}^*, < T_1, T_2, R_1, R_2 >>$ 后，服务器执行以下步骤：

a) 计算 $s' = HD_{sk}(s^*)$；

b) 计算 $B = b^{s'}$，在步骤 4 中会使用该值；

c) 选择随机数 $y \in Z_q^*$ 并计算 $Y = g^y$；

d) 计算 $N_U{}' = HD_{sk}(N_U{}^*)$；

e) 选择随机数 $N_S \in Z_q^*$；

f) 计算

$$V_S = MAC_{\lambda V}(N_U{}', N_S \| \mathrm{GE2OSP}(Y) \| \mathrm{GE2OSP}(X) \| \mathrm{GE2OSP}(T_1) \| \mathrm{GE2OSP}(T_2) \| \mathrm{GE2OSP}(R_1) \| \mathrm{GE2OSP}(R_2))$$

g) 将 $< N_S, Y, V_S >$ 发送给用户。

——步骤 3：当用户收到消息 $< N_S, Y, V_S >$ 时执行如下操作：

a) 验证 V_S，如果不合法则输出 REJECT 并终止协议；

b) 计算 $s_m = r_m + N_S \cdot m(\mathrm{mod}q)$，$s_\gamma = r_\gamma + N_S \cdot \gamma(\mathrm{mod}q)$，$s_k = r_k + N_S \cdot k(\mathrm{mod}q)$，$s_\alpha = r_\alpha + N_S \cdot \alpha(\mathrm{mod}q)$，$s_\mu = r_\mu + N_S \cdot \mu(\mathrm{mod}q)$，$s_\beta = r_\beta + N_S \cdot \alpha \cdot k(\mathrm{mod}q)$；

c) 将 $< s_m, s_\gamma, s_k, s_\alpha, s_\mu, s_\beta >$ 发送回服务器；

d) [可选地计算会话密钥 $\mathrm{SK} = H_\lambda(N_U \| N_S \| \mathrm{GE2OSP}(X) \| \mathrm{GE2OSP}(Y) \| \mathrm{GE2OSP}(Y^{x_1}))$]；

e) 输出 ACCEPT（可选地输出 SK）。

——步骤 4：当收到消息 $< s_m, s_\gamma, s_k, s_\alpha, s_\mu, s_\beta >$ 时，服务器执行以下步骤：

a) 进行如下检验，如果有任何条件不成立输出 REJECT：

1) 检验 $R_2 \cdot (T_2)^{N_S} = g_1{}^{s_\alpha} \cdot g_0{}^{s_\mu}$ 是否成立；

2) 检验 $R_1 \cdot \left(\dfrac{e(T_1,W)}{e(d,h)}\right)^{N_S} = e(T_1,h)^{-s_k} \cdot e(a,h)^{s_m} \cdot e(B,h)^{s_\gamma} \cdot e(g_0,W)^{s_\alpha} \cdot e(g_0,h)^{s_\beta}$ 是否成立。

b) [可选地计算会话密钥 $SK = H_\lambda(N_U' \| N_S \| GE2OSP(X) \| GE2OSP(Y) \| GE2OSP(X^y))$]。

c) 输出 ACCEPT(可选地输出 SK)。

7.2.5 用户撤销

在一个基于辅助存储设施的 PAEA 机制中,用户撤销实际上相当于凭证撤销,在 YZW 机制中,使用动态累加器技术很容易实现整数撤销,在第 7 章中给出了基本的思想。一个动态累加器允许包含很多值的大集合被累加到一个单一累加值中,对于每个累加的值存在一个证据能够表明该值确实在累加值中。该证据可以是零知识的,即不会向检验者揭示任何关于值和证据的信息。动态累加器支持从已存在的累加值中撤销以及往其中添加新值的操作,在更新值时,已存在的证据也需要被更新以保持与新的累加值相一致。

Nguyen 的动态累加器[3]是一个典型的动态累加器技术并可应用于 YZW 机制,通过合并 Nguyen 的动态累加器来扩展 YZW 机制以解决用户撤销问题的基本思想如下:将所有凭证的 k 个值累加到累加值中(用户的凭证为 $< M, m, k, s >$),每个用户在注册完成后都会被颁发一个证据,而 k 和证据都不需被口令包裹凭证保护(即:以明文形式存在)。在用户撤销中的证据更新以及新用户注册遵循在参考文献[3]中定义的相关程序,在用户鉴别操作中,一个用户需要额外地以零知识形式表明用户凭证的 k 值被包含在当前的累加值中。

具体来说,在建立操作中,服务器需要在相同的双线性对 $e: G_1 \times G_2 \rightarrow G_3$ 下为动态累加器机制生成额外的公开参数($W_{acc} = \hbar^{\chi_{acc}}, \hbar \in G_2$)以及秘密的服务器密钥($\chi_{acc} \in Z_q^*$)。在用户注册操作中,服务器计算所有用户的 k 值,并在注册结束时发布累加值 $\Lambda = \hat{g}^{\prod_{j=1}^{n}(k_j + \chi_{acc})}$,其中 $\hat{g}$ 是 Nguyen 动态累加器中的公共参数,n 为注册用户的总数。相应地,将证据 wit_k 连同凭证 $< M, m, k, s >$ 交给用户 U。用户应谨慎地保管由口令保护的凭证中的 wit_k。特别是,由于 wit_k, k 组成了一个可验证对,即 $e(wit_k, W_{acc} \cdot \hbar^k) = e(\Lambda, \hbar)$,所以它们都不能使用口令进行保护;否则,会受到离线猜测攻击。因此其值都要以明文形式存在。综上所述,一个用户的口令保护的凭证为 $cred_{pw} = < M, ENC_{pw}(m'), k, wit_k, HE_{pk}(s) >$。需要注意的是,将 k, wit_k 以明文形式保存不会损害系统的安全性,因为掌握 wit_k, k 并不足以进行鉴别,而且它们只用以担保凭证未被撤销。在匿名鉴别操作中,用户需要额外包含对于 (k, wit_k) 的零知识证明证据,满足 $e(wit_k, W_{acc} \cdot \hbar^k) = e(\Lambda, \hbar)$,其中零知识证明运行如下。注意以下步骤需要和上述原始的匿名鉴别操作协作。

用户首先按照如下步骤计算承诺:

a) 选择随机数 $\zeta, \xi \in Z_q^*$。

b) 计算 $T'_1 = wit_k \cdot g_0^{\zeta}$ 以及 $T'_2 = g_1^{\zeta} \cdot g_0^{\xi}$。

c) 选择随机数 $r_\zeta, r_\eta, r_\xi \in Z_q^*$。

d) 计算 $R'_1 = e(T'_1, \hbar)^{-r_k} \cdot e(g_0, W_{acc})^{r_\zeta} \cdot e(g_0, \hbar)^{r_\eta}$,$R'_2 = g_1^{r_\zeta} \cdot g_0^{r_\xi}$(注意原始匿名鉴别操作中的 r_k 在此处被重复使用)。

e) 将(T'_1, T'_2, R'_1, R'_2)作为承诺发送给服务器。

用户获得服务器挑战消息 $c \in Z_q^*$(即原始匿名鉴别操作中的 N_S)后,执行下面步骤计算响应:

a) $s_\zeta = r_\zeta + c \cdot \zeta (\mathrm{mod} q)$,$s_\xi = r_\xi + c \cdot \xi (\mathrm{mod} q)$,$s_\eta = r_\eta + c \cdot \zeta \cdot k (\mathrm{mod} q)$;

b) 将(S_ζ, S_ξ, S_η)作为响应发送给服务器。

服务器检验响应,若以下检验步骤都通过则输出 Valid,否则输出 Invalid(计算中使用了来自原始匿名鉴别操作的值 s_k)如下:

a) 检验 $R'_2 \cdot (T'_2)^c = g_1^{S_\zeta} \cdot g_0^{S_\xi}$ 是否成立;

b) 检验 $R'_1 \cdot \left(\frac{e(T'_1, W_{acc})}{e(\Lambda, \hbar)}\right)^c = e(T'_1, \hbar)^{-s_k} \cdot e(g_0, W_{acc})^{s_\zeta} \cdot e(g_0, \hbar)^{S_\eta}$ 是否成立。

附 录 A
（规范性附录）
对象标识符

本附录列出了分配给在本部分中描述的机制的对象标识符。

```
AnonymousEntityAuthentication-4 {
iso(1)standard(0) anonymous-entity-authentication(20009) part4(4)
asn1-module(0) algorithm-object-identifiers(0)
}
DEFINITIONS EXPLICIT TAGS::= BEGIN
-- EXPORTS All; --
-- IMPORTS None; --
OID ::= OBJECT IDENTIFIER - alias
-- Synonyms --
is20009-4 OID ::= { iso(1) standard(0) anonymous-entity-authentication(20009)part4(4) }
-- Assignments --
password-only-paea-mechanisms OID ::= { is20009-4 password-only(1) }
storage-extra-paea-mechanisms OID ::= { is20009-4 storage-extra(2) }
-- Password-only PAEA mechanisms --
ski-mechanism OID ::= { password-only-paea-mechanisms ski(1) }
yz-mechanism OID ::= { password-only-paea-mechanisms yz(2) }
-- Storage-extra PAEA mechanisms --
yzw-mechanism OID ::= { storage-extra-paea-mechanisms yzw(1) }
END -- AnonymousEntityAuthentication-4 --
```

参 考 文 献

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

[2] Au M.H., Susilo W., Mu Y. Constant-Size Dynamic k-TAA, Proc. SCN 2006, Lecture Notes in Computer Science, Volume 4116, pp. 111-125,2006.

[3] Nguyen L. Accumulators from bilinear pairings and applications, Proc. CT-RSA'05, Lecture Notes in Computer Science, Volume 3376, pp. 275-292, 2005.

[4] Shin S. H.,Kobara K.,Imai H. On Finding Secure Domain Parameters Resistant to Cheon's Algorithm, IEICE Trans. Fundam. Electron., Commun. Comput. Sci., E98-A (12) pp. 2456-2470, 2015.

[5] Yang J.,&Zhang Z. A New Anonymous Password Based Authenticated Key Exchange Protocol, Proc. INDOCRYPT 2008, Lecture Notes in Computer Science. Volume 5305, pp. 200-212, 2008.

[6] Yang Y.,Zhou J.,Wong J. W.,Bao F.Towards Practical Anonymous Password Authentication, Proc. 26th Annual Computer Security Applications Conference, ACSAC10, pp. 59-68, ACM, 2010.