带系数的离散对数知识签名

姚 前, 陈 舜, 谢 立
(南京大学计算机系, 江苏南京 210008)

摘 要: 知识签名就是签名者在非交互的情况下向别人证明其知道某个秘密而不泄露该秘密本身, 现在知识签名广泛应用在群签名中. 本文主要研究了带系数的离散对数知识签名, 并对几种类型的带系数签名函数进行了定义和证明. 通过对签名函数增加系数, 可以有效地扩大签名函数的选择范围, 增加知识签名的适用性.

关键词: 知识签名; 群签名; 带系数的离散对数知识签名
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2007) 04-0659-04

Signatures of Knowledge of Discrete Logarithm with Coefficient

YAO Qian, CHEN Shun, XIE Li
(Department of Computer Science and Technology, Nanjing University, Nanjing, Jiangsu 210008, China)

Abstract: Signature of knowledge is that signer can prove that he knows knowledge of a secret with respect to public information noninteractively and he don. t leak any secret message. Signature of knowledge has been used in many group signature schemes. In this paper, we mainly study on signature functions of knowledge with coefficient, and give out definition and proof of several kinds of signatures of knowledge of discrete logarithm with coefficient. The coefficient can increase the choices of signature functions, make signatures of knowledge more available.

Key words: signatures of knowledge; group signature; signatures of knowledge of discrete logarithm with coefficient

1 引言

知识签名是一种数学构造, 在这种构造中, 签名者利用数学知识在不泄露某个秘密的情况下向别人证明他知道这个秘密(如 y 以 g 为底的离散对数). 知识签名一般用于秘密内容的证明, 现在广泛应用于群签名[1]中, 从而能有效地确定群成员身份的有效性. 离散对数知识签名的安全性是建立在两个安全假设之上的, 其一: 对于大数 n, 如果不知它因式分解, 对于以 n 为阶的群 G, 在其上计算离散对数是难的; 其二: 已知 i= g^x(mod n), j= g^y(mod n), h= g^{xy}(mod n)的情况下, 对于在 G 中任意选取的(ic, jc, hc), 它与(i, j, h)是难以区分的. 在本文中, 我们为扩大知识签名函数的选择范围、提高其可用性, 在知识签名函数中引入了系数, 并对几种带系数的离散对数知识签名类型进行了定义和证明.

2 背景

2.1 符号与表达式

对于正整数 c, 我们用 c[i]表示其二进制展开的第 i 比特位, 即 c= $\sum_{i\geq 0}$ c[i]#2^i, c[i] ∈ {0, 1}; -, + . 表示串联号; 对于一个集合 A, a ∈ A, 表示 a 属于 A; Z_n 表示模为 n 的整数环; Z_n^* 表示模为 n 的乘法群; H_k(#)为安全散列函数, 其中 k 为安全参数.

2.2 离散对数问题及其变种

设 G 是阶为 n 的乘法群, g 为它的一个生成员, 有 G= <g>, a ∈ Z_n^*, e ∈ Z_n, y ∈ G.

y 以 g 为底的离散对数就是满足等式 y= g^x 的最小正整数 x;

y 以 g, a 为底的双离散对数就是满足等式 y= g^{a^x} 的最小正整数 x;

y 以 g 为底的 e 次方根的离散对数就是满足等式 y= g^{x^e} 的最小正整数 x;

y 以 h, g 为底的表达式离散对数就是满足等式 y= $h^{x_1}g^{x_2}$ 的正整数 x_1, x_2.

以上离散对数, 在不知 n 的因式分解的情况下, 求解它的离散对数是很难的.

3 几种基本的离散对数知识签名

知识签名在文献[2~6]中都有介绍和应用, 本节主要介绍几种基本的基于离散对数的知识签名.

收稿日期: 2006-01-24; 修回日期: 2006-11-05
基金项目: 国家"十五"科技攻关项目(金融示范工程) (No. 2001BA102A04)

311 离散对数的知识签名

设用户 S 的公钥为y, 私钥为 x, 它们满足 $y= g^x$, 其中 g 是G的生成元. 用户 S 对信息m 的签名$(c, s) \in Z/(2^k) \times Z$, 若满足:

$$c= H_k(m+y+g+g^s y^c)$$

其中- + . 为串联号, 称(c, s)为y 关于信息 m 以g 为底的离散对数的知识签名, 并记之为 $SKLOG_k[A: y= g^A](m)$.

312 双离散对数的知识签名

设签名者 S 的公钥为y, 私钥为 x, 它们满足 $y= g^{a^x} \pmod n$, 其中 g 是G 的生成元, $A \in G$, 签名者 S 对信息m 的签名为$(c, s_1, \cdots, s_k) \in Z/(2^k) \times Z^k$, 设:

$$P_i= \begin{cases} g^{A^{s_i}} \pmod n, & \text{若 } c[i]= 0 \\ y^{A^{s_i}} \pmod n, & \text{若 } c[i]= 1 \end{cases}, \quad i= 1, 2, \cdots, k$$

若满足:

$$c= H_k(m+y+g+A+P_1+\cdots+P_k)$$

称$(c, s_1, \cdots, s_k)$为 y 关于信息m 以g、A为底的离散对数的知识签名, 并记之为 $SKLOGLOG_k[B: y= g^{A^B}](m)$.

313 离散对数的 e 次方根的知识签名

设签名者 S 的公钥为y, 私钥为 x, 它们满足 $y= g^{x^e} \pmod n$, 其中 g 是G 的生成元, $e \in Z_n$, 签名者 S 对信息m 的签名$(c, s_1, \cdots, s_k) \in Z/(2^k) \times Z^k$, 设:

$$P_i= \begin{cases} g^{s_i^e} \pmod n, & \text{若 } c[i]= 0 \\ y^{s_i^e} \pmod n, & \text{若 } c[i]= 1 \end{cases}, \quad i= 1, 2, \cdots, k$$

若满足:

$$c= H_k(m+y+g+e+P_1+\cdots+P_k)$$

称$(c, s_1, \cdots, s_k)$为 y 关于信息m 以g 为底的离散对数的e 次方根的知识签名, 并记之为 $SKROOTLOG_k[B: y= g^{\beta^e}](m)$.

314 离散对数表达式的知识签名

设签名者 S 的公钥为y, 私钥为 $x= (x_1, x_2)$, 它们满足 $y= h^{x_1} g^{x_2}$, 其中 g, h 均为 G 的生成员. 签名者 S 对信息m 的签名为$(c, s_1, s_2) \in Z/(2^k) \times Z^2$, 若满足:

$$c= H_k(m+y+g+h+y^c h^{s_1} g^{s_2})$$

称(c, s_1, s_2)为 y 关于信息m 以g、h 为底的离散对数的知识签名, 并记之为:

$$SKREP_k[(A, B): y= h^A g^B](m)$$

4 带系数的知识签名

为扩大知识签名函数的选择范围, 提高知识签名在实际应用中的可用性, 我们在知识签名中引入了系数, 本节将主要讨论几种带系数的知识签名, 并对其进行了证明.

411 带系数的离散对数知识签名

设签名者 S 的公钥为y, 私钥为 x, 它们满足 $y= h^l g^x$, 其中 g, $h \in G$. 而且 g 为G 的生成员, l 是常数且$l \in Z$, 签名者 S 对信息m 的签名为$(c, s) \in Z/(2^k) \times Z$. 若满足

$$c= H_k(m+y+g+h+l+y^c h^{l(1-c)} g^s)$$

称(c, s)为 y 关于信息 m 以 g 为底的以 h^l 为系数的离散对数的知识签名. 并记之为

$$SKCLOG_k[A: y= h^l g^A](m)$$

签名和验证的的具体过程表述如下: 对 $y= h^l g^x$, 当 S 知道x 时

1. 用户 S 对信息m 签名

用户 S 随机选取$r \in Z_n$;

计算 $c= H_k(m+y+g+h+l+h^l g^r)$,

取 $s= r- c \# x \pmod n$

将(c, s)作为 S 对信息m 的签名, 送给验证者 A.

2. 验证者 A 对签名的验证

验证者 A 计算 $cc= H_k(m+y+g+h+l+y^c h^{l(1-c)} \# g^s)$;

若 $c \neq cc$, 拒绝签名;

若 $c= cc$, 表明(c, s)是 y 关于信息 m 以g 为底的以 h^l 为系数的离散对数的知识签名, 即

$$(c, s)= SKCLOG_k[A: y= h^l g^A](m)$$

上述签名过程是一个有效的知识签名, 即(c, s)是 m 的有效数字签名. 证明过程如下:

当 $c= H_k(m+y+g+h+l+y^c h^{l(1-c)} g^s)$ 成立时,

有 $y^c h^{l(1-c)} g^s= (h^l g^x)^c h^{l(1-c)} g^s= h^{lc+l(1-c)} g^{\alpha+s}= h^l g^r$

412 带系数的双离散对数的知识签名

设签名者 S 的公钥为y, 私钥为 x, 它们满足 $y= h^l g^{A^x} \pmod n$, 其中 g 是G 的一生成元, h, $A \in G$, $l \in Z$, l 是一常数, 签名者 S 对信息m 的签名为$(c, s_1, \cdots, s_k) \in Z/(2^k) \times Z^k$. 设

$$P_i= \begin{cases} h^l g^{A^{s_i}} \pmod n, & \text{若 } c[i]= 0 \\ h^{l(1-a^{s_i})} y^{A^{s_i}} \pmod n, & \text{若 } c[i]= 1 \end{cases}, \quad i= 1, 2, \cdots, k$$

若满足

$$c= H_k(m+y+g+A+h+l+P_1+P_2+\cdots+P_k)$$

称$(c, s_1, \cdots, s_k)$为 y 关于信息m 以g、A为底的以 h^l 为系数的双离散对数的知识签名, 并记之为 $SKCLOGLOG_k[B: y= h^l g^{B^A}](m)$.

签名和验证的的具体过程表述如下: 对 $y= h^l g^{A^x}$, 当 S 知道x 时

1. 用户 S 对信息m 签名

用户 S 随机选取$r_1, r_2, \cdots, r_k \in Z_n$;

令: $P_i = h^l g^{A^{r_i}} \pmod n$　　$i = 1, 2, \cdots, k$

计算 $c = H_k(m + y + g + A + h + l + P_1 + P_2 + \cdots + P_k)$

取 $s_i = r_i - c[i] \# x_i \pmod n$　　$i = 1, 2, \cdots, k$

将$(c, s_1, s_2, \cdots, s_k)$作为 S 对信息 m 的签名, 送给验证者 A.

2. 验证者 A 对签名的验证

验证者 A 计算 $cc = H_k(m + y + g + A + h + l + P_1 + P_2 + \cdots + P_k)$;

其中:

$$P_i = \begin{cases} h^l g^{A^{s_i}} \pmod n, & \text{若 } c[i] = 0 \\ h^{l(1 - A^{s_i})} y^{A^{s_i}} \pmod n, & \text{若 } c[i] = 1 \end{cases}, \quad i = 1, 2, \cdots, k,$$

若 $c \neq cc$, 拒绝签名;

若 $c = cc$, 表明$(c, s_1, s_2, \cdots, s_k)$是 y 关于信息 m 以 g, A为底的以 h^l 为系数的双离散对数的知识签名, 即

$$(c, s_1, s_2, \cdots, s_k) = SKCLOGLOG_k[B: y = h^l g^{A^{\beta}}](m)$$

上述签名过程是一个有效的知识签名, 即$(c, s_1, s_2, \cdots, s_k)$是 m 的有效的数字签名, 证明过程如下:

当 $c = H_k(m + y + g + A + h + l + Q_1 + Q_2 + \cdots + Q_k)$;

其中:

$$Q_i = \begin{cases} h^l g^{A^{s_i}} \pmod n, & \text{若 } c[i] = 0 \\ h^{l(1 - A^{s_i})} y^{A^{s_i}} \pmod n, & \text{若 } c[i] = 1 \end{cases},$$

$i = 1, 2, \cdots, k$, 成立时有:

对任意 $i \in [1, \cdots, k]$有以下等式

$$\begin{aligned} Q_i &= \begin{cases} h^l g^{A^{r_i}} \pmod n, & \text{若 } c[i] = 0 \\ h^{l(1 - A^{s_i})} y^{A^{s_i}} \pmod n, & \text{若 } c[i] = 1 \end{cases} \\ &= \begin{cases} h^l g^{A^{(s_i + 0x)}} \pmod n, & \text{若 } c[i] = 0 \\ h^{l(1 - A^{s_i})} (h^l g^x)^{A^{s_i}} \pmod n, & \text{若 } c[i] = 1 \end{cases} \\ &= \begin{cases} h^l g^{A^{r_i}} \pmod n, & \text{若 } c[i] = 0 \\ h^l g^{A^{x + s_i}} \pmod n, & \text{若 } c[i] = 1 \end{cases} \\ &= \begin{cases} h^l g^{A^{r_i}} \pmod n, & \text{若 } c[i] = 0 \\ h^l g^{A^{r_i}} \pmod n, & \text{若 } c[i] = 1 \end{cases} \\ &= P_i \end{aligned}$$

4.1.3　带系数的离散对数的 e 次方根的知识签名

设签名者 S 的公钥为 y, 私钥为 x, 它们满足 $y = h^l g^{x^e} \pmod n$, 其中 g 是 G 的生成元, $h \in G$, $e \in Z_n^*$. $l \in Z$, l 是一常数, 签名者 S 对信息 m 的签名$(c, s_1, \cdots, s_k) \in Z/(2^k) @ Z^k$. 设

$$P_i = \begin{cases} h^l g^{s_i^e} \pmod n, & \text{若 } c[i] = 0 \\ h^{l(1 - s_i^e)} y^{s_i^e} \pmod n, & \text{若 } c[i] = 1 \end{cases}, \quad i = 1, 2, \cdots, k,$$

若满足

$$c = H_k(m + y + g + e + h + l + P_1 + P_2 + \cdots + P_k)$$

称$(c, s_1, \cdots, s_k)$为 y 关于信息 m 以 g 为底的以 h^l 为系数的离散对数的 e 次方根的知识签名, 并记之为 $SKC2ROOTLOG_k[B: y = h^l g^{B^e}](m)$

签名和验证的的具体过程表述如下: 对 $y = h^l g^{x^e}$, 当 S 知道 x 时

1. 用户 S 对信息 m 签名

用户 S 随机选取 $r_1, r_2, \cdots, r_k \in Z_n$;

令: $P_i = h^l g^{r_i^e} \pmod n$　　$i = 1, 2, \cdots, k$

计算 $c = H_k(m + y + g + e + h + l + P_1 + P_2 + \cdots + P_k)$

取 $s_i = r_i / x^{c[i]} \pmod n$　　$i = 1, 2, \cdots, k$

将$(c, s_1, s_2, \cdots, s_k)$作为 S 对信息 m 的签名, 送给验证者 A.

2. 验证者 A 对签名的验证

验证者 A 计算 $cc = H_k(m + y + g + e + h + l + P_1 + P_2 + \cdots + P_k)$; 其中:

$$P_i = \begin{cases} h^l g^{s_i^e} \pmod n, & \text{若 } c[i] = 0 \\ h^{l(1 - s_i^e)} y^{s_i^e} \pmod n, & \text{若 } c[i] = 1 \end{cases}, \quad i = 1, 2, \cdots, k,$$

若 $c \neq cc$, 拒绝签名;

若 $c = cc$, 表明$(c, s_1, s_2, \cdots, s_k)$是 y 关于信息 m 以 g 为底的以 h^l 为系数的离散对数的 e 次方根的知识签名, 即

$$(c, s_1, s_2, \cdots, s_k) = SKCROOTLOG_k[B: y = h^l g^{B^e}](m)$$

上述签名过程是一个有效的知识签名, 即$(c, s_1, s_2, \cdots, s_k)$是 m 的有效的数字签名, 证明过程如下:

当 $c = H_k(m + y + g + e + h + l + Q_1 + Q_2 + \cdots + Q_k)$, 其中:

$$Q_i = \begin{cases} h^l g^{s_i^e} \pmod n, & \text{若 } c[i] = 0 \\ h^{l(1 - s_i^e)} y^{s_i^e} \pmod n, & \text{若 } c[i] = 1 \end{cases}, \quad i = 1, 2, \cdots, k,$$

成立时有:

对任意 $i \in [1, \cdots, k]$有以下等式

$$\begin{aligned} Q_i &= \begin{cases} h^l g^{s_i^e} \pmod n, & \text{若 } c[i] = 0 \\ h^{l(1 - s_i^e)} y^{s_i^e} \pmod n, & \text{若 } c[i] = 1 \end{cases} \\ &= \begin{cases} h^l g^{(s_i * 1)^e} \pmod n, & \text{若 } c[i] = 0 \\ h^{l(1 - s_i^e)} (h^l g^{x^e})^{s_i^e} \pmod n, & \text{若 } c[i] = 1 \end{cases} \\ &= \begin{cases} h^l g^{(s_i * x^0)^e} \pmod n, & \text{若 } c[i] = 0 \\ h^l g^{(x * s_i)^e} \pmod n, & \text{若 } c[i] = 1 \end{cases} \\ &= \begin{cases} h^l g^{r_i^e} \pmod n, & \text{若 } c[i] = 0 \\ h^l g^{r_i^e} \pmod n, & \text{若 } c[i] = 1 \end{cases} \end{aligned}$$

$= P_i$

4.4 带系数的表达式知识签名

设签名者 S 的公钥为 y, 私钥为 $x=(x_1, x_2)$, 它们满足 $y=h^l g_1^{x_1} g_2^{x_2}$, 其中 $g_1, g_2, h \in G$. g_1, g_2 是 G 的生成员, 签名者 S 对信息 m 的签名为 $(c, s_1, s_2) \in Z/(2^k) \times Z^2$, 若满足:

$$c=H_k(m+y+g_1+g_2+h+l+h^{l(1-c)} g_1^{s_1} g_2^{s_2})$$

称 (c, s_1, s_2) 为 y 关于信息 m 以 g_1、g_2 为底的以 h^l 为系数的表达式知识签名, 并记之为 $SKCREP_k[(A, B): y=h^l g_1^A g_2^B](m)$.

签名和验证的的具体过程表述如下: 对 $y=h^l g_1^{x_1} g_2^{x_2}$, 当 S 知道 $x=(x_1, x_2)$ 时

1. 用户 S 对信息 m 签名

用户 S 随机选取 $r_1, r_2 \in Z_n$;

计算 $c=H_k(m+y+g_1+g_2+h+l+h^l g_1^{r_1} g_2^{r_2})$

取 $s_i=r_i-c\#x_i \pmod n \quad i=1, 2$

将 (c, s_1, s_2) 作为 S 对信息 m 的签名, 送给验证者 A.

2. 验证者 A 对签名的验证

验证者 A 计算 $cc=H_k(m+y+g_1+g_2+h+l+y^c h^{l(1-c)} g_1^{s_1} g_2^{s_2})$;

若 $c \neq cc$, 拒绝签名;

若 $c=cc$, 表明 (c, s_1, s_2) 是 y 关于信息 m 以 g 为底的以 h^l 为系数的离散对数的知识签名, 即:

$$(c, s_1, s_2)=SKCREP_k[(A, B): y=h^l g_1^A g_2^B](m)$$

上述签名过程是一个有效的知识签名, 即 (c, s_1, s_2) 是 m 的有效数字签名, 证明过程如下: 当 $c=H_k(m+y+g_1+g_2+h+l+y^c h^{l(1-c)} g_1^{s_1} g_2^{s_2})$ 成立时,

有 $y^c h^{l(1-c)} g_1^{s_1} g_2^{s_2}=(h^l g_1^{x_1} g_2^{x_2})^c h^{l(1-c)} g_1^{s_1} g_2^{s_2}$

$$= h^l g_1^{cx_1+s_1} g_2^{cx_2+s_2}= h^l g_1^{r_1} g_2^{r_2}$$

5 总结

在这篇文章里, 我们主要研究了带系数的离散对数知识签名, 对几种带系数的离散对数知识签名类型进行了定义和证明. 带系数的离散对数知识签名可以扩大知识签名函数的选择范围, 便于系统实现中的函数选择, 可广泛应用于各类群签名应用环境.

参考文献:

[1] D Chaum, E van Heyst. Group signatures[A]. In: Advances in Cryptology2EUROCRYPT. 91[C]. LNCS 950. Springer2Verlag, 1992. 257- 265.

[2] G Ateniese, J Camenisch, M Joye, G Tsudik. A practical and provably secure coalition2resistant group signature scheme[A]. In: Advances in Cryptology CRYPTO. 2000[C]. LNCS 1880. Springer2Verlag, 2000. 255- 270.

[3] G Ateniese, D Song, G Tsudik. Quasi2efficient revocation of group signatures[A]. In: Financial Cryptography(FC 02)[C]. LNCS 2357. Springer2Verlag, 2002. 183- 197.

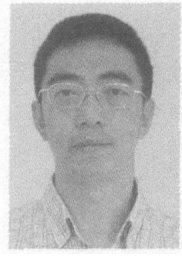
[4] G Ateniese, B de Medeiros. Efficient group signatures without trapdoors[A]. In: ASIACRYPT 2003[C]. Springer2Verlag, 2003. 246- 268.

[5] J Camenisch, M Stadler. Effient group signature schemes for large groups[A]. In: Advances in Cryptology2CRYPTO. 97[C]. LNCS 1294. Springer2Verlag, 1997. 410- 424.

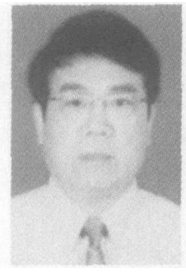
[6] D X Song. Practical forward secure group signature schemes[A]. In: Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS 2001)[C]. ACM press, 2001. 225- 234.

作者简介:

姚 前 男, 1970 年 6 月出生于安徽歙县, 南京大学计算机系博士生, 主要研究方向为分布式系统和计算机安全.
E2mail: qyao@chinaclear. com. cn



陈 舜 男, 1964 年 2 月出生于云南镇雄, 南京大学计算机系博士, 主要研究方向为分布式系统和计算机安全.
E2mail: chenshun@csrc. gov. cn



谢 立 男, 1942 年 4 月出生于江苏常熟, 南京大学计算机系教授, 博士生导师, 主要研究方向为分布式计算、并行处理、先进操作系统等.
E2mail: xieli@nju. edu. cn