基于 GF(q^N) 上秩距离码的校验矩阵的验证方案 [1]

杜伟章 王新梅

(西安电子科技大学综合业务网国家重点实验室 西安 710071)

摘 要 J.Stern(1996) 在 "公钥验证的一个新范例" 中基于 GF(2) 上纠错码的校验矩阵提出了一验证方案. 该文基于 GF(q^N) (q 为素数) 上秩距离码的校验矩阵提出一新的验证方案, 将 J. Stern 的方案中对秘密数据 s 的重量限制改为对 s 的秩的限制; 证明了在随机预言模型中给出的协议是零知识交互证明, 并显示出通过参数的适当选取, 此方案比 J. Stern 的方案更安全.

关键词 验证方案, 校验矩阵, 秩距离码, 零知识

中图号 TN918.1

1 引 言

验证方案是一密码协议, 它使得团体 A("证明者") 对团体 B("检验者") 多项式多次地证明他的身份, 而 B 无法对其他人冒称它自己为 A . 验证方案能通过使用零知识交互证明系统做到, 1985 年 S. Goldwasser , S. Micali 和 C. Rackoff 在文献 [1] 中提出了零知识交互证明的思想.

J.Stern 在文献 [2] 中基于二元域上纠错码的校验矩阵提出了一验证方案, 本文基于 GF(q^N) (q 为素数) 上秩距离码的校验矩阵提出了一新的验证方案. 秩距离码的含义见文献 [3] .

文中的验证方案涉及如下有限域上秩距离码的伴随式译码问题, 将此问题称为 "SD" 问题.

名词: SD

输入: $H(m,n)$ 为 GF(q^N) 上 $[n, n-m, d]$ 秩距离码 Π 的校验矩阵, i 为 GF(q^N) 上一长度为 m 的 q 元向量.

问题: 是否存在 GF(q^N) 上长度为 n 秩为 p 的向量 s , 使得 $i = Hs$.

2 方案的描述

此验证方案依赖委托与杂凑函数的概念 (见文献 [2]) , 文中要求杂凑函数是免于碰撞的. 下面用小写字母表示向量, 大写字母表示矩阵, 所有运算都是在 GF(q^N) 上进行的; 文中符号 $y \cdot \sigma$, $< x >$, $M^T(y^T)$, $\overline{A}$, $\tilde{A}$, A , $\overline{B}$, $\tilde{B}$, (X,Y), $(X,Y)[I]$ 的含义见文献 [2,4] .

文中的方案使用 GF(q^N) 上一固定的 $(m \times n)$ 阶矩阵 H . 此矩阵是对所有用户公开的, 且首先由一大家都信赖的中心随机地构造.

在登记后, 每个用户 U 收到一秘密钥 s , s 的秩为 p , 由中心随机地选择. 用户的公开身份为 $i = Hs$.

前后关系如下:

公共的公开数据: $H(m,n)$ 为 GF(q^N) 上秩为 m 的矩阵, 一个标为 $< \cdot >$ 的杂凑函数;

证明者的秘密数据: s 为 GF(q^N) 上长度为 n 的向量;

证明者的公开数据: $i = Hs$, 且 s 的秩为 p .

[1] 1999-10-19 收到, 2000-04-07 定稿
高等学校博士学科点专项科研基金资助课题 (批准号: 98070104)

设 A 要向 B 证明他的身份，协议包括 r 轮，每轮执行如下：

(1) 证明者选择 $\mathrm{GF}(q^N)$ 上长度为 n 的向量 y 连同整数集合 $\{1,2,\cdots,n\}$ 的随机置换 σ，把委托 c_1, c_2, c_3：

$$c_1 =< \sigma//H(y) >, c_2 =< y\cdot\sigma >, c_3 =< (y+s)\cdot\sigma >$$

送给检验者。在此背景下 c_1 中的置换 σ 看作是一个向量，并注意到 $y\cdot\sigma$ 指的是 y 在置换 σ 下的像；

(2) 检验者送属于 $\{0,1,2\}$ 的随机元素 b；

(3) 如果 b 是 0，证明者显示 y 和 σ；如果 b 是 1，证明者显示 $(y+s)$ 和 σ；如果 b 是 2，证明者显示 $y\cdot\sigma$ 和 $s\cdot\sigma$；

(4) 如果 b 是 0，检验者检查 c_1 和 c_2；如果 b 是 1，检验者检查 c_1 和 c_3，注意 $H(y)=H(y+s)+(q-1)i$；如果 b 是 2，检验者检查 c_2 和 c_3 且检查 $s\cdot\sigma$ 是否满足 s 所满足的条件。

3 方案的性质

下面描述方案所具有的性质。

令 $I=\{H,i,p\}$ 是 A 和 B 共享的公开数据，且令 $P(I,w)$ 是如下谓词：

$p(I,w)=$ “ w 为一 s，s 满足 $i=Hs$，且 s 的秩为 p；H，i，$p\in I$ ”，则有如下结论：

引理 1 如果 $\overline{B}$ 带有大于等于 $(2/3)^r+\varepsilon$ 的概率接受 $\tilde{A}$ 的证明，则存在一多项式时间概率机 M，带有压倒优势的概率，或者计算出一合法的秘密的 s 或找到对杂凑函数的一个碰撞。

证明 令 T 是当对手有一随机带 R_A 时，$(\tilde{A},\overline{B})$ 相应于检验者所有可能问题的执行树。在每个阶段，$\overline{B}$ 可问 3 个可能的问题。首先将显示，除非一个杂凑碰撞已经被找到，一个秘密钥 s 能从一带有 3 个儿子的顶点计算出。然后将显示存在多项式时间概率图灵机 M 带有压倒优势的概率能找到 T 中那样的一个顶点。

令 V 是一带有 3 个儿子的顶点，这相应于 3 个委托 c_1, c_2, c_3 被计算以及 3 个询问被适当地回答的情况。令 y_0 和 σ_0 是对询问 $b=0$ 的回答；w_1 和 σ_1 是对询问 $b=1$ 的回答；和 z_2，t_2 是对询问 $b=2$ 的回答。则有

$$< \sigma_0//H(y_0) >= c_1 =< \sigma_1//H(w_1)+(q-1)i > \tag{1}$$

$$< y_0\cdot\sigma_0 >= c_2 =< z_2 > \tag{2}$$

$$< w_1\cdot\sigma_1 >= c_3 =< z_2+t_2 >,\quad t_2\text{的秩为 } p \tag{3}$$

这样，或者一个对杂凑函数的碰撞已经被找到，或者由 (1) 式有

$$\sigma_0=\sigma_1 \tag{4}$$

$$H(y_0)=H(w_1)+(q-1)i \tag{5}$$

由 (2) 式有

$$y_0\cdot\sigma_0=z_2 \tag{6}$$

由 (3) 式有

$$w_1 \cdot \sigma_1 = z_2 + t_2 \tag{7}$$

令 $\sigma_0 = \sigma_1 = \sigma$，由 (5) 推出 $i = H(w_1) + (q-1)H(y_0)$ 成立。这样

$$i = H[(q-1)y_0 + w_1] \tag{8}$$

$$y_0 \cdot \sigma = z_2 \tag{9}$$

$$w_1 \cdot \sigma = z_2 + t_2 \tag{10}$$

由 (9) 式和 (10) 式，得

$$[(q-1)y_0 + w_1] \cdot \sigma = (q-1)z_2 + (z_2 + t_2) = t_2 \tag{11}$$

则由 (11) 式和 t_2 的秩为 p 可知 $[(q-1)y_0 + w_1]$ 的秩也为 p，这样推出 $[(q-1)y_0 + w_1]$ 是一合法的秘密钥，能被用来模仿 $\overline{A}$。

现在，引理的假设隐含 T 有一个带有 3 个儿子的顶点的概率至少为 ε。确实，考虑 R_A 为一 μ 个元素的集合，$\tilde{A}$ 从中随机地选择它的值，令 Q 是集合 $\{0,1,2\}$。这两个集合都看作是带有均匀分布的概率空间。

设 $(c,b)(\in (R_A \times Q)^r)$ 表示在验证过程期间 $\tilde{A}$ 和 $\tilde{B}$ 之间交换的委托、询问和回答。如果 $(\tilde{A}, \overline{B})$ 的执行导致成功状态，则称 (c,b) 是一合法对。

令 V 是由所有合法对组成的 $(R_A \times Q)^r$ 的子集，引理的假设意味着

$$\frac{|V|}{|(R_A \times Q)^r|} \geq [2/3]^r + \varepsilon \tag{12}$$

此处 $|A|$ 表示集合 A 中元素的个数。

令 Ω_r 是 R_A^r 的一子集使得

(1) 如果 $c \in \Omega_r$，则 $2^r + 1 \leq |\{b, (c,b)\text{是合法的}\}| \leq 3^r$；

(2) 如果 $c \in R_A^r \backslash \Omega_r$，则 $0 \leq |\{b, (c,b)\text{是合法的}\}| \leq 2^r$，有 $V = \{\text{合法的}(c,b),\ c \in \Omega_r\} \cup \{\text{合法的}(c,b),\ c \in R_A^r \backslash \Omega_r\}$，因此

$$|V| \leq |\Omega_r| 3^r + (\mu^r - |\Omega_r|) 2^r \tag{13}$$

由 (13) 式有

$$\frac{|V|}{|(R_A \times Q)^r|} \leq \left[\frac{|\Omega_r|}{|R_A^r|} + 2^r \left(3^{-r} - \frac{|\Omega_r|}{|(R_A \times Q)^r|}\right)\right] \leq \frac{|\Omega_r|}{|R_A^r|} + \left(\frac{2}{3}\right)^r \tag{14}$$

由 (12) 式和 (14) 式得出

$$\frac{|\Omega_r|}{|R_A^r|} \geq \varepsilon \tag{15}$$

(15) 式显示出入侵者通过选择随机的值，可回答检验者询问的至少 $2^r + 1$ 次的概率大于 ε。现在，如果多于 $2^r + 1$ 次询问被一入侵者通过，则 T 至少有 $2^r + 1$ 片叶子，即 T 至少有一带有 3 个儿子的顶点。所以，由 $\tilde{A}$ 的重放 $\lceil 1/\varepsilon \rceil$ 次，并再加一次重复，则可以任意接近于 1 的概率找到一带有 3 个儿子顶点的执行树。　　证毕

定理 1　此协议是对 $P(I,w)$ 的交互的知识证明。

证明 (1) 完备性：明显地，对公开的数据 I，知道一有效 s 的每个证明者能正确地回答 B 的询问．这样有 $\Pr((\overline{A},\overline{B})[I]=$ "成功" $)=1$．

(2) 完善性：引理 1 的第 1 个结论隐含 $<\cdot>$ 不是免于碰撞的，第 2 个结论与此 SD 问题在多项式时间的不可行性矛盾．由此得出 $\Pr((\tilde{A},\overline{B})[I]=$ "成功" $)\le[2/3]^r$．这样证明了此协议是对 $P(I,w)$ 的交互的知识证明． 证毕

下面我们来证明在随机预言模型中此协议是对 $P(I,w)$ 的零知识交互证明．用 $R_{A,B}$ 表示在一验证过程期间 A 与 B 之间交换的所有 bit 的级联，称它为 (A,B) 的通信带．因为交互协议的概率性质，在 $R_{A,B}$ 上定义了一概率分布，则可得如下结论．

定理 2 在随机预言模型中此协议是对 $P(I,w)$ 的零知识交互证明．

证明 用 $x//y$ 表示串 x 和 y 的级联．为了模仿一不诚实的检验者，模仿者针对证明者送的委托，设计一特别的策略．令 $S(c_1,c_2,c_3)$ 是那样一个策略，我们有 $S(c_1,c_2,c_3)\in\{0,1,2\}$．考虑 $\phi_s:\ F_{q^N}^n\to F_{q^N}^n,\ \ y\mapsto y+s$; $\psi:\ F_{q^N}^n\to F_{q^N}^m,\ \ y\mapsto H(y)$; 则 ϕ_s 是 $F_{q^N}^n$ 到 $F_{q^N}^n$ 的一一映射．

下面的 M 是一多项式时间概率图灵机，它产生一通信带，此通信带的概率分布与由一令人满意的验证过程产生的通信带的概率分布是不可区分的．

(1) M 随机地选择属于 $\{0,1,2\}$ 的一询问 b．

(a) 如果 $b=0$，M 选择：u 为属于 $F_{q^N}^n$ 的随机元素；σ 为 $\{1,2,\cdots,n\}$ 的任一置换．和计算 $c_1=<\sigma//H(u)>, c_2=<u\cdot\sigma>$ 且用一随机串代替 c_3．令 $F=c_1//c_2//c_3$ 和 $E=u//\sigma$．很明显 u 和 y 有同样的概率分布在随机预言模型中，$u\cdot\sigma$ 和 $y\cdot\sigma$ 有同样的概率分布．

(b) 如果 $b=1$，M 选择：u 为属于 $F_{q^N}^n$ 的随机元素；σ 为 $\{1,2,\cdots,n\}$ 的任一置换，和计算 $c_1=<\sigma//H(u)+(q-1)i>, c_3=<u\cdot\sigma>$ 且用一随机串代替 c_2．令 $F=c_1//c_2//c_3$ 和 $E=u//\sigma$；很明显 u 和 $(y+s)$ 有同样的概率分布，事实上，令 z 是 $F_{q^N}^n$ 的任意元素，由于 y 是 $F_{q^N}^n$ 的随机元素，有

$$\Pr(y+s=z)=\Pr(y=\phi_s^{-1}(z))=(q^N)^{-n}=\Pr(u=z)$$

(c) 如果 $b=2$，M 选择：u 为属于 $F_{q^N}^n$ 的随机元素；s' 为 $F_{q^N}^n$ 中秩为 p 的任意元素；σ 为 $\{1,2,\cdots,n\}$ 的任意置换．和计算 $c_2=<u\cdot\sigma>$，$c_3=<(u+s')\cdot\sigma>$ 且用一随机串代替 c_1．令 $F=c_1//c_2//c_3$ 和 $E=u\cdot\sigma//s'\cdot\sigma$；很明显 $u\cdot\sigma$ 和 $y\cdot\sigma$ 有同样的概率分布，而且 $(u+s')$ 和 $(y+s)$ 有同样的概率分布．实际上，$(u+s')$ 和 u 有同样的概率分布，$(y+s)$ 和 y 有同样的概率分布，这样 $(u+s')$ 和 $(y+s)$ 有同样的概率分布．

(2) M 计算 $b'=S(F)$．

(3) 如果 $b'=b$，则 M 在带 $\Re$ 上写下量 F，b 和 E，否则 M 回到步骤 (1)．

这样，平均地在 $3r$ 轮内，M 产生一通信带 $\Re$，$\Re$ 与由在 r 轮内执行的一令人满意的验证过程产生的通信带 $R_{A,B}$ 是不可区分的．由此证明了在随机预言模型中所讨论的协议是对 $P(I,w)$ 的零知识交互证明． 证毕

4 方案的安全性

下面讨论一下方案的安全性．很清楚，此方案的安全依赖由 $H(s)$ 求 s 的困难性 (当它的变量被限制为有效的秘密钥时)．根据组合论，秩为 p 的 n 维向量的总数为 $[(q^n-1)\cdots(q^n-$

$q^{p-1}) \times (q^N-1)\cdots(q^N-q^{p-1})]/[(q^p-1)\cdots(q^p-q^{p-1})] \approx q^{p(n+N)-p^2}$，而 GF(2) 上长度为 n，重量为 p 的向量的总数为 C_n^p，可以看出通过 p 的适当选取，秩为 p 的 n 维向量的总数比 C_n^p 大得多，这样如果采取穷搜索的方法进行攻击，该方案比文献 [2] 中的方案安全些．另外，由于秩为 p 的 n 维向量的总数近似为 $q^{p(n+N)-p^2}$，它随 n 指数增长，这样如果采取穷搜索的方法，将使工作因子变得很大．最后，如果由方程 $i=Hs$ 找秩为 p 的解 s，由文献 [5]，对此秩距离码的一般译码问题需 $O((np+N)^3q^{(N-p)(p-1)})$ 次初等运算，通过 n, p, N, q 的选取，可使此运算在计算上不可行．而如果直接求解方程 $i=Hs$ 找秩为 p 的解，由于方程 $i=Hs$ 有 $(q^N)^{n-m}$ 个解，当 $n-m$ 较大时，对解进行穷搜索在计算上是不可行的．这样就证明了此方案在计算上的安全性．

不知道秘密钥，为了伪造一给定的身份，可应用下述各种策略：

(1) 对检验者的询问仅仅准备了 y 和 σ，而对各委托的计算用秩为 p 的某任意向量 t 代替未知的 s．这时假的证明者希望 b 是 0 或 2．在第 1 种情况，他能显示 y 和 σ，在第 2 种情况，他归还 $y\cdot\sigma$ 和 $t\cdot\sigma$，而当 $b=1$ 时他不能回答．从而成功的概率是 $[2/3]^r$，这里 r 是轮数．

(2) 对检验者的询问仅仅准备了 $(y+s)$ 和 σ，而对各委托的计算用秩为 p 的任意向量 t 代替未知的 s．这时假的证明者希望 b 是 1 或 2．在第 1 种情况，他能显示 $(y+s)$ 和 σ; 在第 2 种情况，他归还 $(y+s+(q-1)t)\cdot\sigma$ 和 $t\cdot\sigma$; 而当 $b=0$ 时，他不能回答．从而成功的概率是 $[2/3]^r$，这里 r 是轮数．

(3) 对检验者的询问准备了 y 和 $(y+t)$，这里 t 是不同于 s 并满足 $H(t)=i$，且秩不为 p 的某元素，而对各委托的计算用 $\{1,2,\cdots,n\}$ 的任一置换 σ' 代替 σ．这时假的证明者希望 b 是 0 或 1．在第 1 种情况，他显示 y 和 σ'; 在第 2 种情况，他显示 $(y+t)$ 和 σ'; 而当 $b=2$ 时他不能回答．从而成功的概率是 $[2/3]^r$，这里 r 是轮数．

这样当 r 充分大时，对手成功的概率很小．

5 方案的空间复杂性与通信复杂性

下面介绍文中方案的空间复杂性与通信复杂性．如文献 [2] 中一样，也不需储存 H 的全部，仅储存某些选择位置的字即可，然后由一固定的软件随机数产生器扩展它，这样可知该方案的空间复杂性为文献 [2] 中方案的空间复杂性的 $\lceil \ln q/\ln 2 \rceil$ 倍．而协议的通信复杂性为文献 [2] 中方案的 N 倍，这样仍然可用智能卡实现．

6 结 束 语

文中基于最大秩距离码的伴随式译码问题，提出了一种新的验证方案，由于文中所提出的 SD 问题是一 NP 完全问题，可证明通过参数的适当选取，它比文献 [2] 中的方案更安全．该方案存在的问题为它的通信复杂性比文献 [2] 中的方案的通信复杂性高．

参 考 文 献

[1] S. Goldwasser, S. Micali, C. Rackoff, The knowledge complexity of interactive proof-systems, SIAM Journal on Computing, 1989, 18(1), 186–208.

[2] J. Stern, A new paradigm for public key identification, IEEE Trans. on Information Theory, 1996, 42(6), 1757–1768.

[3] E. M. Gabidulin, Theory of codes with maximum rank distance, Problems of Information Transmission, 1985, 21(1), 1–12.

[4] U. Feige, A. Fiat, A. Shamir, Zero knowledge proofs of identity. Journal of Cryptology, 1988, 1(2), 77–94.

[5] F. Chabaud, J. Stern, The cryptographic security of the syndrome decoding problem for rank distance codes, Advances in Cryptology-Asiacrypt'96 (K.Kim, T. Matsumoto, eds.), Lecture Notes in Computer Science, Vol.1163, Berlin, Springer-Verlag, 1996, 368–381.

AN IDENTIFICATION SCHEME BASED ON PARITY CHECK MATRIX OF RANK DISTANCE CODES OVER GF(q^N)

Du Weizhang Wang Xinmei

(*National Key Lab of Integrated Service Networks, Xidian Univ., Xi'an* 710071, China)

Abstract An identification scheme based on parity check matrix of error-correcting codes over GF(2) was proposed in the paper "A New Paradigm for Public Key Identification" by J. Stern(1996), a new identification scheme based on parity check matrix of rank distance codes over GF(q^N) (q is a prime) is proposed in this paper, the limitation on the weight of mysterious datum s is changed into the limitation on the rank of s. It is proved that the given protocol is a zero-knowledge interactive proof in the random oracle model, and it is shown that the scheme is more secure than the scheme of J. Stern when parameters are selected properly.

Key words Identification scheme, Parity check matrix, Rank distance code, Zero-knowledge

杜伟章: 女，1965 年生，讲师，博士生，研究方向为通信与密码学，主要从事秩距离码与认证码方面的研究工作.

王新梅: 男，1937 年生，博士生导师，教授，主要从事信道编码、密码学、通信网络安全方面的研究工作. 已在国内外学术刊物上发表论文 80 余篇，出版学术专著 5 部.