基于变量组合的 REESSE1-E 签名方案

苏盛辉[1],吕述望[2]
(1.北京工业大学计算机学院,北京 100124; 2.中国科学院研究生院,北京 100039)

摘 要: 文章介绍了互素序列的定义和杠杆函数的概念,描述了 REESSE1-E 签名方案的密钥生成、数字签名和身份验证三个算法,证明了验证算法的正确性,示范了如何利用变量之间的组合来构造难题.文章从五个主要方面分析了签名与验证的安全性,它包括从公钥推导私钥、从签名码提取私钥、仅通过公钥伪造签名码、通过已知签名码和公钥伪造另一个签名码以及通过选择消息伪造签名码等.分析表明基于变量组合的 REESSE1-E 签名方案的安全性等价于离散对数难题.

关键词: 签名方案; 安全性; 变量组合; 离散对数问题; 杠杆函数
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2010) 01-0234-05

REESSE1-E Public-Key Signature Scheme Based on Variable Combination

SU Sheng-hui[1], LÜ Shu-wang[2]
(1. *School of Computer, Beijing University of Technology, Beijing* 100124, *China*;
2. *School of Graduate, Chinese Academy of Sciences, Beijing* 100039, *China*)

Abstract: Presents the definition of a coprime sequence and the concept of the lever function, elaborates the three algorithms of the REESSE1-E public-key signature scheme for key generation, digital signature and identity verification, proves the correctness of the verification algorithm, and illustrates how the hardnesses are constructed by means of variable combination. The paper analyzes the security of the REESSE1-E against inferring a private key from a public key, extracting a private key from a signature, and faking a signature only through a public key, through known signatures with a public key, or through chosen messages, which manifests that the lowest security of REESSE1-E based on variable combination is equivalent to the discrete logarithm problem.

Key words: signature scheme; security; variable combination; discrete logarithm problem; lever function

1 引言

1999 年,TTM 多变量公钥密码体制被提出[1],它的安全性基于小域上多变量柔性自同构问题.2002 年,基于类似思想的 TTS 多变量签名体制被提出[2].

2001 年至 2003 年间,笔者相继提出了 REESSE1 和 REESSE2 两个公钥密码体制[3,4],与单一变量的 RSA 和 ElGamal 体制[5,6]不同(单变量性是指私钥中任何一个变量的暴露都会使体制土崩瓦解),它们具有多变量的特点.目前,并没有关于多变量密码学(Multivariate cryptography)或多变量密码体制(Multivariate cryptosystems)的一个明确定义,不过,从文献[1~4]来看,多变量密码体制应该具有这些特征:

(1)私钥和公钥各是一组变量,相应地,存在一组密钥变换式,或者说,从私钥到公钥的变换是一个联立方程组.

(2)每个变换可以是多项式的,也可以是非多项式的,例如,幂指函数的,关键在于保证较强的安全性和正确的解密.

(3)私钥的变量个数可以多于公钥的变量个数,函数的可逆性很差,即使泄露部分私钥也不能推导出全部私钥.

(4)由于变量较多,变量之间的组合形式较多,因此,多变量体制具有较大的改进空间.

多变量签名正如量子有序签名一样[7],为我们迎接未来的挑战提供了一种新的选择.

本文提出的基于变量组合的 REESSE1-E 签名方案与早期的 REESSE1 签名完全不同.我们将分析其私钥安全性大于离散对数难题(Discrete Logarithm Problem, DLP)、其签名安全性等价于 DLP.透过 REESSE1-E,本文揭示了多变量与变量组合之间以及变量组合与难题形成之间的一种关系.

收稿日期:2008-04-25;修回日期:2009-11-08
基金项目:国家 863 高技术研究发展计划(No.2009AA01Z441);国家 973 重点基础研究发展规划(No.2007CB311100)

在本文,符号 gcd 代表最大公约数,%代表模运算,$\|x\|$代表 $x\%M$ 的阶,$|Y|$代表集合 Y 的大小,$\bar{M}$ 表示 $(M-1)$.

2　互素序列与杠杆函数

定义 1　如果 A_1、A_2、…、A_n 为 n 个互不相同、两两互素且大于 1 的整数,则称这一整数系列为互素序列,记为$\{A_1,\cdots,A_n\}$,简记为$\{A_i\}$.

性质 1　对于任意正整数 $m\leqslant n$,从互素序列$\{A_i\}$中任选 m 个项组成子集$\{A_{x_1},\cdots,A_{x_m}\}$,则子集的连乘积 $G=A_{x_1}\cdots A_{x_m}$ 是唯一确定的,即 G 与$\{A_{x_1},\cdots,A_{x_m}\}$一一对应. G 也称为互素序列乘积.

证明见文献[3].

本签名体制中,密钥变换式为 $C_i\equiv(A_i\ W^{\ell(i)})^G(\%M)$,其中,指数 $\ell(i)$被称为杠杆函数,下面给出关于它的一个描述性定义.

定义 2　在一个公钥体制中,密钥变换式中的参数 $\ell(i)$被称为杠杆函数,如果它具有下述特点:

(1)$\ell(\cdot)$是整数到整数的单射函数,其定义域为$[1,n]$,值域为$(1,M)$.令 $\mathscr{L}_n$ 代表从定义域到值域的所有单射的集合,则 $\ell(\cdot)\in\mathscr{L}_n$,且$|\mathscr{L}_n|\geqslant A_n^n=n(n-1)\cdots1$.

(2)变量 i 与 $\ell(i)$间的映射关系随机确定,无解析表达式,故每次公钥生成时,$\ell(\cdot)$不一样.

(3)在密钥变换式中,不存在从 $\ell(\cdot)$到公钥的专门映射.

(4)从公钥推导私钥时,不得不考虑序列$\{\ell(1),\cdots,\ell(i)\}$的全排列,故当 n 足够大时,全排列在有效时间内不可穷举.

(5)从私钥解开密文时,只需要考虑序列$\{\ell(1),\cdots,\ell(i)\}$的累加和,其时间复杂度与 n 多项式相关,故解密是可行的.

显然,$\ell(\cdot)$是在"公开"一端计算量大,在"私有"一端计算量小.

3　REESSE1-E 签名方案的设计

3.1　密钥生成算法

设 S、$T\geqslant2^n$ 为互素的整常数.

(1)随机产生长度为 n 的互素序列$\{A_1,\cdots,A_n\}$;

(2)找到素数 M 满足 $T^2|\bar{M}$、$\gcd(S,\bar{M})=1$,计算 $G\leftarrow\prod_{i=1}^{n}A_i\%M$;

(3)选择整数 $\delta<M$ 使得$\|\delta\|/\gcd(\|\delta\|,T)\geqslant2^n$;

(4)计算 $\alpha\leftarrow\delta^{ST}\%M$,$W\leftarrow(\alpha\delta^{-\delta^\delta})^{S^{-1}}G^{-G}\%M$;

(5)产生两两不同的杠杆值 $\ell(1),\cdots,\ell(n)\in\Omega=\{5,\cdots,n+4\}$;

(6)计算序列$\{C_1,\cdots,C_n\,|\,C_i\leftarrow(A_iW^{\ell(i)})^G(\%M)\}$.

最后,以($\{C_i\}$、α)作为公钥,($\{A_i\}$、$\{\ell(i)\}$、W、δ)作为私钥. S、T、M 共用.

注意:寻找阶为 k 的某元素 x,先计算 $x\equiv c^{\bar{M}/k}(\%M)$,$c<M$ 为任意整数,然后,利用文献[9]中 1.4 节的算法 1.4.4 或文献[10]中 4.6 节的算法 4.80 来进一步测试 x.

集合 $\Omega=\{5,\cdots,n+4\}$不是唯一的,例如,可以选择奇数集合 $\Omega=\{5,7,\cdots,2n+3\}$.

3.2　数字签名算法

设'¬'为比特的求反运算.

设($\{A_i\}$、$\{\ell(i)\}$、W、δ)为私钥,F 为待签文件或消息,Hash 为杂凑函数.

(1)令 $H\leftarrow$Hash(F),其二进制形式为 $b_1\cdots b_n$;

(2)计算 $G\leftarrow\prod_{i=1}^{n}A_i\%M$,$k_1\leftarrow G\sum_{i=1}^{n}b_i\ell(i)\%\bar{M}$,$G_0\leftarrow\prod_{i=1}^{n}A_i^{\neg b_i})^G\%M$;

(3)任选 R,计算 $Q\leftarrow(RWG_0)^{HS}\delta\%M$,$U\leftarrow(RW^{k_1})^{QHT}\delta^{\delta TR}\%M$;

(4)计算 $V\leftarrow\delta RU+r\%\bar{M}$,其中 r 满足 $QU+Sr\equiv\delta^\delta HQU(\%\bar{M})$.

算法执行后,得到数字签名码(Q、U、V),其可随文件 F 一起发送给验证者.

由于 $\gcd(S,\bar{M})=1$,根据定理 1,计算 r 是容易的.

注意:R 不允许被重复产生(见 4.2 节).

设 p 为素数.

定理 1　设 $x^n\equiv a(\%p)$、p 为素数,如果 $\gcd(n,p-1)=1$,则每一个 a 恰好有一个模 p 的 n 次根.特别,令 $\mu\equiv n^{-1}(\%p-1)$,那么($a^\mu\%p$)是 a 模 p 的一个 n 次根.

定理 2　设 $x^n\equiv a(\%p)$、p 为素数,如果 $n|(p-1)$ 且 $\gcd(n,(p-1)/n)=1$,则当 a 是一个 n 次幂剩余时,($a^\mu\%p$)是 a 模 p 的一个 n 次根,这里,$\mu\equiv n^{-1}(\%(p-1)/n)$.

定理 1 和 2 的证明见文献[11]中 12 章.

注意:通过定理 1 和 2 求出的解称为 $x^n\equiv a(\%p)$ 的平凡解.即能够在确定多项式时间内求出的、用 a 的幂次表示的解[12].

3.3　身份验证算法

设($\{C_i\}$、α)为公钥,F 为待签文件或消息,(Q、U、V)为其签名码.

(1)令 $H\leftarrow$Hash(F),其二进制形式为 $b_1\cdots b_n$;

(2)计算 $\hat{G}\leftarrow\prod_{i=1}^{n}(C_i)^{b_i}\%M$;

(3)计算 $X\leftarrow(\alpha^{H}Q^{-1})^{TQU}\%M$,

$Y\leftarrow(\hat{G}^{TQU}U^{-1})^{SU}\alpha^{V}\%M$;

(4)若 $X\equiv Y\neq 1$,则签名有效且 F 未被修改,否则,身份无效或 F 在传输中已被修改.

算法执行后,可以达到鉴别签名真伪、防发送者抵赖和抗攻击者修改的目的.

3.4 身份验证算法的正确性

下面,对验证算法中的判别式 $X\equiv Y(\%M)$做一推导,有关推导在交换群$(\mathbb{Z}_M^*,\cdot)$中进行[13].从 3.1 和 3.2 节知

$$\alpha\equiv\delta^{ST}\equiv\delta^{\delta^{\delta}}(W(\prod_{i=1}^{n}A_i)^{G})^{S}(\%M).$$

令 $\Lambda\equiv(R^{-1}G_1)^{QUH}\delta^{r}(\%M)$,其中 $G_1(\prod_{i=1}^{n}A_i^{b_i})^{G}$ 且 $G_0G_1\equiv(\prod_{i=1}^{n}A_i)^{G}(\%M)$,则

$$\begin{aligned}Q^{QU}\Lambda^{S}&\equiv(RWG_0)^{HSQU}\delta^{QU}(R^{-1}G_1)^{QUHS}\delta^{rS}\\&\equiv(WG_0G_1)^{HSQU}\delta^{QU+rS}\\&\equiv(WG_0G_1)^{HSQU}\delta^{\delta^{\delta}HQU}\\&\equiv(\delta^{\delta^{\delta}}(WG_0G_1)^{S})^{HQU}\\&\equiv(\alpha)^{HQU}(\%M).\end{aligned}$$

移项得 $\Lambda^{S}\equiv(\alpha^{H}Q^{-1})^{QU}(\%M)$,从而,

$$\Lambda^{ST}\equiv(\alpha^{H}Q^{-1})^{QUT}\equiv X(\%M)$$

又

$$\begin{aligned}U^{U}\Lambda^{T}&\equiv(RW^{k_1})^{HTQU}\delta^{\delta TRU}(R^{-1}G_1)^{QUHT}\delta^{rT}\\&\equiv(W^{k_1}G_1)^{HTQU}\delta^{\delta TRU+rT}\\&\equiv\hat{G}^{HTQU}\delta^{T(\delta RU+r)}\\&\equiv\hat{G}^{HTQU}\delta^{TV}(\%M)\end{aligned}$$

移项得 $\Lambda^{T}\equiv(\hat{G}^{HTQ}U^{-1})^{U}\delta^{TV}(\%M)$,从而,

$$\Lambda^{ST}\equiv(\hat{G}^{HTQU}U^{-1})^{SU}\delta^{STV}\equiv(\hat{G}^{HTQU}U^{-1})^{SU}\alpha^{V}\equiv Y(\%M).$$

因此,有 $\Lambda^{ST}\equiv X$ 和 $\Lambda^{ST}\equiv Y(\%M)$.

根据双同余定理,得到 $X\equiv Y(\%M)$.

定理 3 (双同余定理) 设 p 为素数,s、t 满足 $\gcd(s,t)=1$为整常数,则联立方程 $x^{s}\equiv a(\%p)$、$x^{t}\equiv b(\%p)$有唯一解的充要条件是 $a^{t}\equiv b^{s}(\%p)$.

证明见文献[14].

4 REESSE1-E 签名方案的安全性分析

4.1 从公钥推导私钥是比 DLP 更困难的

私钥安全是最根本的安全.如果私钥不安全,则必定有签名码的不安全.

首先,考察 $C_i\equiv(A_iW^{\prime(i)})^{G}(\%M)$,其中,$G\in(1,M)$,$\prime(\cdot)$具有不确定性[8].

假设 $\bar{A}\equiv A_iW^{\prime(i)}(\%M)$是一个常数,则 $C_i\equiv\bar{A}^{G}(\%M)$归约到 DLP.但实际上 $\bar{A}\in(1,M)$不是一个常数,因此,求解 $C_i\equiv(A_iW^{\prime(i)})^{G}(\%M)$是比 DLP 更困难的,它被称为多变量排列难题[14].

另外,$A_i^{G}\in(1,M)$不是小整数,因此,利用连分式方法从$\{C_i\}$推导$\{A_i\}$也是不可行的[8].

其次,考察 $\delta^{ST}\equiv\alpha(\%M)$,它相当于 $\delta^{T}\equiv\alpha^{S-1}(\%M)$.

由于 $T^2\mid\bar{M}$、$\gcd(T,\bar{M}/T)=T$,因此,用定理 2 无法直接求得 δ 的平凡解.

如果两边同时 T 次方,则有 $\delta^{T^2}\equiv(\alpha^{S-1})^{T}(\%M)$.根据子群的性质,$\delta^{T^2}\equiv(\alpha^{S-1})^{T}(\%M)$之平凡解同时为 $x^{T}\equiv\alpha^{S-1}(\%M)$之平凡解的概率仅为 $1/T$[12].

若根据文献[9]的概率算法 1.6.1 找到 $x^{T}\equiv\alpha^{S-1}(\%M)$的一个随机解,则其时间复杂度为 $O(\max(2^{T-1},\bar{M}/T))$[9,11].当 $T>80$ 或 $\bar{M}/T>2^{80}$时,该算法无效.

如果企图用离散对数方法[10,15]求得 $x^{T}\equiv\alpha^{S-1}(\%M)$的一个解 x_0,则 x_0 恰好等于 δ 的概率为 $1/T<1/2^{n}$.这说明在离散对数时间内亦不能找到 δ.最后,考察

$$\alpha\equiv\delta^{\delta^{\delta}}(W(\prod_{i=1}^{n}A_i)^{G})^{S}\equiv\delta^{\delta^{\delta}}(WG^{G})^{S}(\%M).$$

由于 W、δ 和 G 均未知,因此,从 α 推知 W、δ 或 G 是不确定的和不可能的.

4.2 从签名码推导私钥至少是指数时间问题

从签名算法知:$Q\equiv(RWG_0)^{HS}\delta(\%M)$、$U\equiv(RW^{k_1})^{HTQ}\delta^{\delta TR}(\%M)$和 $V\equiv\delta RU+r(\%-1)$.

当攻击者欲求 RWG_0 时,相当于解同余方程 $x^{HS}\equiv Q\delta^{-1}(\%M)$.

由于 δ 未知,因此,无法求出 $x\equiv RWG_0(\%M)$.又从密钥生成算法知$\|\delta\|/\gcd(\|\delta\|,T)\geqslant 2^{n}$,即$\|\delta\|\geqslant 2^{n}$.因此,若猜测 δ,则猜中 δ 的概率为 $1/\|\delta\|\leqslant 1/2^{n}$.

当攻击者欲求 RW^{k_1}时,相当于解同余方程 $x^{HTQ}\equiv U\delta^{-\delta^{\delta}TR}(\%M)$.

由于 $\gcd(HTQ,\bar{M})\geqslant T$,因此,如果 $\delta^{-\delta^{\delta}TR}$被猜中,则方程可能存在平凡解.但平凡解等于 RW^{k_1}的概率小于或等于 $1/T\leqslant 1/2^{n}$.退一步,即使 RW^{k_1}被找到,由于 $R\in(1,\bar{M})$的任意性,W^{k_1}不能被确定.

对于 $V\equiv\delta RU+r(\%\bar{M})$,有 $r\equiv V-\delta RU(\%\bar{M})$.进而,有

$$QU+S(V-\delta RU)\equiv\delta^{\delta}HQU(\%\bar{M})$$

如果允许 R 重复,则可以找到两组签名(Q_1、U_1、V_1)和(Q_2、U_2、V_2)满足上式,从而可以求出 δR 和 δ^{δ}.但由于已经规定 R 不能重复,因此,求出 δR 和 δ^{δ} 是不可行的.

又 $Q\equiv(RWG_0)^{HS}\delta(\%M)$,如果以 $R\equiv(Q\delta^{-1})^{1/(HS)}$

$(WG_0)^{-1}(\%M)$代入上式(假设 $H^{-1}\%\bar{M}$ 存在),则得

$$QU + S(V - Q\delta^{-1})^{1/(HS)}(WG_0)^{-1}\delta U) \equiv \delta^{\delta}HQU(\%\bar{M})$$

可以找到同一个消息的两组签名代入上式,得到一个关于$(WG_0)^{-1}\delta^{1-1/(HS)}$和 δ^{δ} 的联立方程组,即使求出$(WG_0)^{-1}\delta^{1-1/(HS)}$和 δ^{δ},但从它们中继续求出 δ、W 和 G_0 在离散对数时间内是不可行的.

如果猜测 W 或$\delta \in (1,\bar{M})$,则猜中的概率为 $1/M \leqslant 1/2^n$.

所以,从数字签名码得到私钥至少是 $O(2^n)$指数时间问题.

4.3 仅从公钥伪造签名码是个难题

4.3.1 从验证算法伪造签名码至少是 DLP

超对数问题:设 p 为素数,$g \in (\mathbb{Z}_p^*,\cdot)$为生成元,且 a、b、$c \in (\mathbb{Z}_p^*,\cdot)$满足 $a^a \equiv c(\%p)$和 $g^b \equiv c(\%p)$,则从 $x^x \equiv c(\%p)$求 a 是困难的,且比从 $g^x \equiv c(\%p)$求 b 更困难.

超对数问题的时间复杂度分析见文献[14].

设 H 为文件 F 的 Hash 值,$(Q、U、V)$为其签名码,则判别式

$$(\alpha^H Q^{-1})^{TQU} \equiv (\hat{G}^{HTQU}U^{-1})^{SU}\alpha^V(\%M)$$

即 $X \equiv Y$ 成立.其中 α 为公钥,$\hat{G}$ 从$\{C_i\}$和 H 可以求出.

三个变量,一个方程,因此,可以假设两个变量的值.如果假设 Q、V 的值且 U 存在,求 U 是超对数问题.如果假设 U、V 的值且 Q 存在,则求 Q 是超对数问题.如果假设 Q、U 的值且 V 存在,则求 V 是离散对数问题.

特别,令 $Q \equiv \alpha^H(\%M)$和 $U \equiv \hat{G}^{HTQ}(\%M)$,则 $\alpha^V \equiv 1(\%M)$,进而可以 $V = \bar{M}$,即$(\alpha^H、\hat{G}^{HTQ}、\bar{M})$为一个伪造的签名.因此,我们在判别式中不允许 $X = 1$ 和 $Y = 1$.

4.3.2 从签名算法伪造签名码等价于 DLP

从签名算法来看,因为 $Q \equiv (RWG_0)^{HS}\delta(\%M)$、$U \equiv (RW^{k_1})^{HTQ}\delta^{\delta TR}(\%M)$和$V \equiv \delta RU + r(\%\bar{M})$,攻击者可以尝试下列攻击方法.

首先,利用求离散对数的 Index-calculus 方法[10],解高阶同余方程 $x^T \equiv \alpha^{1/S}(\%M)$,求出 x.注意,x 等于 δ 的概率仅为 $1/T$.

令 $Q \equiv (a)^{HS}x(\%M)$、$U \equiv (b)^{HTQ}x^{xTR}(\%M)$和 $\Lambda \equiv (c)^{HQU}x^r(\%M)$,又令 $QU + Sr \equiv yHQU(\%\bar{M})$.则

$$\begin{aligned} Q^{QU}\Lambda^S &\equiv (a)^{HSQU}x^{QU}(c)^{HSQU}x^{rS} \\ &\equiv (ac)^{HSQU}x^{QU+rS} \\ &\equiv (ac)^{HSQU}x^{yHQU} \\ &\equiv (x^y(ac)^S)^{HQU}(\%M) \end{aligned}$$

假设 a、c 的值,令 $x^y(ac)^S \equiv \alpha(\%M)$,则在离散对数时间内可以求出 y.

令 $bc \equiv \hat{G}(\%M)$,可以求出 b.

假设 R 的值,可以求出 Q、U.进一步,根据 $QU + Sr \equiv yHQU(\%\bar{M})$可以求出 r.又

$$\begin{aligned} U^U\Lambda^T &\equiv (b)^{HTQU}x^{xTRU}(c)^{HTQU}x^{rT} \\ &\equiv (bc)^{HTQU}x^{xTRU+rT} \\ &\equiv (\hat{G})^{HTQU}x^{T(xRU+r)} \\ &\equiv (\hat{G})^{HTQU}x^{T(xRU+r)}(\%M) \end{aligned}$$

令 $V \equiv xRU + r(\%\bar{M})$.则$(Q、U、V)$被伪造出.

上述分析表明,根据签名算法和公钥来伪造签名码等价于离散对数问题.

4.4 从已知签名码和公钥伪造另一个签名码至少是 DLP

给定文件 F 和其签名$(Q、U、V)$,并假设存在另一个文件 F'及其相应的H'和$\hat{G}'$,那么,如果任何$(Q'、U'、V')$满足

$$(\alpha^{H'}Q'^{-1})^{TQ'U'} \equiv (\hat{G}'^{H'TQ'}U'^{-1})^{SU'}\alpha^{V'}(\%M)$$

则它是关于 F'的一个伪造签名.

已知签名 $Q、U、V$ 的值应该被利用.

如果令 $Q' = Q、V' = V$,则无论 U'是否存在,求 U'是超对数难题.

如果令 $U' = U、V' = V$,则无论 Q'是否存在,求 Q'是超对数难题.

如果令 $Q' = Q、U' = U$,则无论 V'是否存在,求 V'是离散对数难题.

如果已知多个三元组$(Q、U、V)$,则数据分析表明多个 Q 之间、U 之间或 V 之间没有统计规律(是由 R 的随机性带来的),且从对 ElGamal 签名算法的分析知[10],它们对求解离散对数问题也是没有帮助的.

因此,从已知签名和公钥伪造另一个签名至少是离散对数难题.

4.5 选择签名的伪造攻击至少是 DLP 难题

由于 $H = b_1 \cdots b_n$,$\hat{G} \equiv \prod_{i=1}^{n} C_i^{b_i}(\%M)$,因此,$H$ 与 $\hat{G}$ 之间无多项式的表达关系.

从判别式$(\alpha^H Q^{-1})^{TQU} \equiv (\hat{G}^{HTQ}U^{-1})^{SU}\alpha^V(\%M)$知

$$(\alpha\hat{G}^{-S})^{HTQU} \equiv (U^{-1})^{SU}\alpha^V(Q)^{QUT}(\%M)$$

假设 $Q、U、V$ 的值,并猜测 $\hat{G}$ 的值,则从上式求取 H 是 DLP 问题,并且 $\hat{G} \equiv \prod_{i=1}^{n} C_i^{b_i}(\%M)$的概率小于 $1/2^n$.

又从判别式知

$$\hat{G}^{-HSTQU} \equiv (\alpha^H Q^{-1})^{TQU}(U)^{SU}\alpha^{-V}(\%M)$$

假设 $Q、U、V$ 的值,由于 H 未知,从上式求取 $\hat{G}$ 是困难的.即使 $\hat{G}$ 被求出,从 $\hat{G}$ 推知 H 是比 DLP 问题更困难的[14].

5 跋

本文提出的 REESSE1-E 签名方案虽然用到了三个难题:多变量排列难题、超对数难题和离散对数难题,但根据木桶原理(木桶盛水的多少取决于最短的那块木板),它的安全性仍然只是等价于离散对数问题的.因此,如果要把它用到实践中,其模数 M 的长度至少应该为 512 比特或 1024 比特.由于 REESSE1-E 签名方案的模数长度与 ElGamal 相当,因此,两者的运行速度、即计算复杂度也是相当的.

Hash 算法中的无碰撞压缩函数对 Hash 算法的安全性仅是必要的而不是充分的[16].如果 Hash 算法是采用传统的 Merkle-Damgård 迭代结构[10],则考虑到生日攻击[10],消息摘要 H 的比特长度一般是 $2n$,因此,建议采用一种新型的 3C 迭代结构[16],该迭代结构中的压缩函数仍然可以来自 MD5、SHA-0 或 SHA-1 等,这样,消息摘要 H 的比特长度为 n 即可.

REESSE1-E 签名方案也属于多难题公钥密码体制.多难题公钥体制必定是多变量公钥体制,因为只有多变量才能带来多难题.反过来,多变量不一定带来多难题.同时,我们也发现,多变量之间不同的组合,可以导致不同复杂度的难题,因而带来不同的安全性.这正是 REESSE1-E 签名方案的理论价值所在.

需要说明的是,我们在本文中没有给出方案安全性的形式化证明,而只是给出了其精确安全性分析.针对体制全部或部分安全需求的可证安全被 Goldreich 等人倡导[17],但是,当一个理想的随机 Oracle 被任何一个实际的函数取代时,某些在随机 Oracle 模型下被证明是安全的加密或签名方案被发现是不安全的[18],另外,Koblitz 和 Menezes 等学者在"Another Look at 'Provable Security'"一文中也对可证安全提出了批评,认为可证安全是更加适合于密码协议的[19].

参考文献:

[1] T Moh. On Tame Transformation Method (TTM)[OL]. http://www.usdsi.com/lctr.ps,1999.

[2] Jiun-ming Chen, Bo-yin Yang. Tame transformation signatures with topsy-turvy hashes[A]. Proc. of the IWAP '02[C]. Taipei,2002.

[3] 苏盛辉.REESSE1 公开密钥密码体制[J].计算机工程与科学,2003,25(5):13 - 16.

[4] 苏盛辉,杨炳儒.REESSE2 公开密钥密码体制[J].计算机科学,2004,31(9):148 - 151.

[5] R L Rivest, A Shamir, L M Adleman. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM,1978,21(2):120 - 126.

[6] T ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory,1985,31(4):469 - 472.

[7] 温晓军,刘云.一种可实现的量子有序多重数字签名方案[J].电子学报,2007,35(6):1079 - 1083.

[8] 苏盛辉,杨义先,杨炳儒.REESSE1 加密方案中杠杆函数的充要性分析[J].电子学报,2006,34(10):1892 - 1895.

[9] Henri Cohen. A Course in Computational Algebraic Number Theory[M]. Berlin: Springer-Verlag,2000, ch.1,3.

[10] A J Menezes, P Van Oorschot, S Vanstone. Handbook of Applied Cryptography[M]. London: CRC Press,1997, ch.4,9.

[11] Paul Garrett. Making, Breaking Codes: An Introduction to Cryptology[M]. New Jersey: Prentice-Hall,2001, ch.12.

[12] Shenghui Su, Shuwang Lü. To Solve the High Degree Congruence x^n = a (mod p) in GF(p)[A]. The Proceedings of 2007 International Conference on the Computational Intelligence and Security[C]. IEEE Computer Society Press, Dec,2007.672 - 676.

[13] Thomas W Hungerford Algebra[M]. New York: Springer-Verlag,1998, ch.1.

[14] 苏盛辉.多变量和不确定性公钥密码体制的研究[D].北京:北京科技大学博士论文,2007.03.

[15] Song Y Yan. Number Theory for Computing[M]. 2nd ed., Berlin: Springer-Verlag,2002, ch.1.

[16] P Gauravaram, W Millan, E Dawson etc. Constructing secure hash functions by enhancing merkle-damgärd construction [A]. Australasian Conference on ISP[C]. Springer-Verlag, 2006.407 - 420.

[17] Oded Goldreich. Foundations of Cryptography: Basic Tools [M]. Cambridge, UK: Cambridge University Press,2001, ch.4.

[18] Ran Canetti, Oded Goldreich, Shai Halevi. The random oracle methodology revisited[A]. Proceedings of the 30th ACM STOC'98[C]. New York: ACM Press,1998.209 - 218.

[19] Neal Koblitz, Alfred J. Menezes. Another look at "Provable Security"[J]. Journal of Cryptology,2007,20(1):3 - 37.

作者简介:

苏盛辉 男,博士,北京工业大学计算机学院教授.分别就读于国防科大、北京大学和北京科大.自 2000 年以来主导提出 REESSE 系列密码体制,获国家发明专利权 3 项.研究兴趣:算法复杂性、公钥密码和信息安全. E-mail: sheenway@126.com

吕述望 男,中国科学院研究生院教授,博导,SMS4 对称体制首席发明人,中国科技大学毕业.自 1982 年以来一直从事密码体制的研究,获国家奖励多项.研究兴趣:密码算法和信息安全.