第 31 卷第 2 期　　电 子 与 信 息 学 报　　Vol.31No.2
2009 年 2 月　　Journal of Electronics & Information Technology　　Feb. 2009

一个安全的广义指定验证者签名证明系统

陈国敏　　陈晓峰
(中山大学计算机科学系　广州　510275)

摘　要：广义指定验证者签名(UDVS) 可以实现任意的签名持有者能向任意的验证者证明签名者确实签署了该签名，而且验证者没有能力向第三方证明该签名是有效的。这种签名方案可以保护签名持有者的隐私信息，因而在证书系统中有着重要的应用。然而，UDVS 需要签名持有者(designator)与指定的验证者(designated-verifier)通过签名者(signer)的公钥体系来生成自己的密钥对，这在现实情况下是不合理的。最近，Baek 等人(2005)在亚洲密码会提出 UDVSP (Universal Designated Verifier Signature Proof)来解决这个问题。该文首先指出 Baek 等人所给出的 UDVSP 协议存在一个安全性缺陷，即不满足 UDVS 系统中的不可传递性(non-transferability)，然后提出一种新的 UDVSP 协议，并证明该方案满足所定义的安全属性。

关键词：广义指定验证者签名证明；双线性对；承诺协议
中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1009-5896(2009)02-0489-04

A New Secure Universal Designated Verifier Signature Proof System

Chen Guo-min　　Chen Xiao-feng
(*Department of Computer Science*, *Sun Yat-sen University*, *Guangzhou* 510275, *China*)

Abstract: The notion of Universal Designated Verifier Signature (UDVS) allows any holder of a signature to convince any designated verifier that the signer indeed generated the signature without revealing the signature itself, while the verifier can not transfer the proof to convince anyone else of this fact. Such signature schemes can protect the privacy of signature holders and have applications to certification systems. However, they require the designated verifier to create a public key using the signer's public key parameter and have it certified to ensure the resulting public key is compatible with the setting that the signer provided. This is unrealistic in some situations. Very recently, Baek *et al* introduced the concept of Universal Designated Verifier Signature Proof (UDVSP) to solve this problem in Asiacrypt 2005. In this paper, it is first showed that there exits a security flaw in this UDVSP, *i.e.*, it does not satisfy the non-transferability. A new secure UDVSP system is proposed and the system is proved to achieve the desired security notions.

Key words: Universal Designated Verifier Signature Proof (UDVSP); Bilinear pairings; Commitment protocol

1　引言

近几年来很多学者力图解决现有数字签名中认证性和隐私性之间的冲突。Chaum 和 Van Antwerpen[1]首次提出了不可否认性数字签名的概念，它可以让签名者决定什么时候他或她的签名可以被验证。在另一些情况中，让签名者决定的不仅有特定的时间而且还有特定的人才能验证该数字签名是很重要的。这就是指定验证者签名[2](DVS)提出的动机。近年来，许多学者对不可否认签名及指定验证者签名进行了大量的研究，并给出了许多高效的方案[3−7]。

Steinfeld 等人[8]首次在 2003 年亚洲密码会提出了有关广义指定验证者签名(UDVS)的概念，这种方案可以看成是对 DVS 的延伸，以解决类似以下例子的信用问题：假设 Alice 是 A 大学的毕业生，她想去 B 公司找工作，负责面试她的考官 Bob 要验证她是否拿到 A 大学的毕业证，而 Alice 却不想让除 Bob 外的人知道自己获得了 A 大学的学位或者没有证据说明她获得了 A 大学的学位。由于一般的数字签名满足广义可验证性，所以很难实现 Alice 的要求。而广义指定验证者签名(UDVS)可以解决这个问题。但 Steinfeld 等人[8]的方案有个缺点是签名持有者(designator 在上例中指的是 Alice)要与指定的验证者(designated verifier 在上例中指的是考官 Bob)要通过签名者(signer 在这里指的是学校 A)的公钥体系来生成自己的公钥和私钥，这样就有个成本问题(可以想像，公司 B 面对的可能不是一个学校的学生，这就需要存储并计算数量巨大的公钥和私钥，带来巨大的成本，很多公司可能负担不起)，如果指定的验证者(desinated-verifier 在上例中指的是考官 Bob)不合作，那么这种数字签名机制就不

2007-09-29 收到，2008-04-14 改回
国家自然科学基金(60503006)和中韩国际合作研究基金(60611140543)资助课题

能有效地进行，从而使该签名的效率不高。

Baek 等人[9]在 2005 年亚洲密码会提出了广义指定验证者签名证明(UDVSP)协议来解决这个问题。 UDVSP 可以使指定的验证者(designated-verifier 在上例中指的是考官 Bob)省去生成密钥的成本，大大提高该签名系统的效率。他通过设计一个签名持有者和指定的验证者之间的交互式协议(interactive protocol)来实现要求。然而，Baek 等人所给出的 UDVSP 协议存在一个安全性缺陷，即不满足原来 UDVS 中的不可传递性(non-transferability)。

UDVSP 中所用到的零知识证明协议是一个基于诚实验证者的交互式零知识证明协议，然而在 UDVSP 中，验证者一般是不诚实的，那么他使用 Fiat-Shamir [10] 的方法可以容易地将之转化成一个非交互式零知识证明协议。所以一个不诚实的验证者可以得到一个证据向其它验证者证明这是原始签名者的签名，从而不满足 UDVS 中的不可传递性。一般来说，无收据的电子投票系统，无滥用的电子合同方案中也存在这样的问题。

本文提出一个新的安全的广义指定验证者签名证明系统，该系统不仅满足 UDVSP 所具有的性质，而且它和 UDVS 一样满足不可传递性，从而最大程度上保护了用户的隐私。本文方案的主要思想是使用一个比特承诺方案[11]来构造一个真正的交互式的零知识证明协议，从而满足不可传递性。所以，本文的主要贡献有两点：(1)指出 Baek 等人所提出的两个 UDVSP 系统不满足不可传递性，所以它不能达到 UDVS 所具有的安全性。(2)提出一个新的满足不可传递性的 UDVSP 系统，该系统可以安全代替 UDVS 使用。

2 预备知识

2.1 双线性对(Bilinear pairings)[12]

令 G_1 是一个阶为素数 q 的加法群， G_2 是一个阶为 q 的循环乘法群，双线性对是指满足下列性质的一个映射 e：

(1)双线性：对任意的 $P,Q,r \in G_1, a,b \in {}_RZ_q^*$， $e(aP,bQ) = e(P,Q)^{ab}$。

(2)非退化性：对任意的 $P \in G_1$， 存在 $Q \in G_1$， 使得 $e(P,Q) \neq 1$。

(3)可计算性：对所有的 $P,Q \in G_1$， 存在有效的算法 $e(P,Q)$。

定义 1 离散对数问题(DLP)：给定 2 个群元素 P,Q 计算整数 n， 使得 $Q = nP$。

定义 2 判定 Diffie-Hellman 问题(DDHP)：对 $a,b,c \in {}_RZ_q^*, P \in G_1$ 而言，给定 P,aP,bP,cP 判定 $c = ab \bmod q$。

定义 3 计算 Diffie-Hellman 问题(CDHP)：对 $a,b,c \in {}_RZ_q^*, P \in G_1$ 而言，给定 P,aP,bP,cP， 即计算 abP。

在群 G_1 中，当 DDHP 容易计算但 CDHP 计算困难时，称 G_1 为 Gap Diffie-Hellman (GDH) 群。同时，我们假定 G_1 和 G_2 上的 DLP 和 CDHP 都是困难的。GDH 群能在有限域上的超奇异椭圆曲线或超椭圆曲线上找到，而双线性对可由 Weil 对和 Tate 对获得。

定义 4 OMDL 问题(OMDLP)：“One more Discrate Logarithm”的概念是由 Bellare[13]提出的。这个问题的过程可以描述如下：

Experiment：令 $SP = (q,p,e,G_1,G_2,k)$ 为系统参数。有一个多项式时间的攻击者 A m 次询问挑战预言 $C(.)$， n 次询问挑战预言 $DL(.)$。令 $(s_1,s_2,\cdots,s_n) \leftarrow A^{C(.),DL_{p,q}(.)}(SP)$。

Output：如果 $(g^{s_1} = h_1) \wedge \cdots \wedge (g^{s_m} = h_m)$，并且 $n < m$，则返回 1，反之，返回 0。(其中 $h_1,h_2,\cdots,h_m$ 为挑战预言 $C(.)$ 的输出)。

2.2 Bit 承诺协议[11]

A 想向 B 承诺未来发生的一个事件预测值 b，但在事件出现前不对 B 泄露；另一方面要使 B 确信 A 对他所做出的承诺不会改变。通常的承诺协议包括两个过程：

承诺生成：

(1) A 生成两个随机数 R_1 和 R_2。

(2) A 将 R_1 和 R_2 及承诺消息 b 组成 (R_1,R_2,b)。

(3) A 计算 (R_1,R_2,b) 的单向函数值 $H(R_1,R_2,b)$，并随机选择一个数 R_1， 将 $(H(R_1,R_2,b), R_1)$ 送给 B。

承诺兑现：

(4) A 将 (R_1,R_2,b) 送给 B。

(5) B 计算 (R_1,R_2,b) 的单向杂凑值，并与(3)中收到的值相比较。同时还将(4)中的 R_1 与(3)中收到的 R_1 比较，如果一致，证明 A 的承诺合法。

2.3 UDVSP 的定义与性质

UDVSP 的概念是由 Baek 等首先提出的，方案由 5 个多项式-时间算法和一个交互式协议组成：

SigKenGen：用一个安全的参数 $k \in N$ 作为输入，产生签名者的系统公钥/私钥对 (pk,sk)。该算法可以写成：$(pk,sk) \leftarrow \text{SigKeyGen}(k)$。

Sign：用签名者的私钥 sk 和一个消息 m 作为输入，产生一个对 m 的签名 σ。该算法可以写成：$\sigma \leftarrow \text{Sign}(sk,m)$。

Verify：用签名者的公钥 pk， m 的签名 σ 和消息 m 作为输入，如果签名 σ 对消息 m 是有效的则输出 1，否则输出 0。该算法可以写成 $d \leftarrow \text{Verify}(pk,\sigma,m)$， 其中 $d \in \{0,1\}^*$

Tranform：用签名者的公钥 pk， m 的签名 σ 作为输入，基于 pk 选择一个秘密参数 $s\tilde{k}$，用 $s\tilde{k}$ 将 σ 转化为 $\tilde{\sigma}$。该算法可以写成 $(s\tilde{k},\tilde{\sigma}) \leftarrow \text{Tranform}(pk,\sigma)$。

IVerify：这是一个在签名持有者(定义为 P)和指定验证者 (定义为 V) 之间的交互式验证协议。

UDVSP 满足的性质：

(1)不可伪造性：签名在适应性选择消息攻击下不能被伪造[14]。这个一般由所使用的签名方案达到。

(2)UDVSP 可以抵抗假冒攻击：UDVSP 能阻止没有持有有效签名的攻击者假冒诚实的指定验证者。假冒攻击可以

被分为 2 类：Type-1 和 Type-2 攻击。在 Type-1 攻击中，攻击者已经获得了一个转化过的签名，他以签名持有者的身份参与到与指定验证者的交互式协议中，试图假冒诚实的签名持有者。在 Type-2 攻击中，攻击者完全忽视他之前得到的转化过的签名，而是试图自己重新生成一个签名，并用这个签名来和指定验证者进行交互，冒充诚实的签名持有者。对 Type-1 和 Type-2 攻击的正式定义请参考文献[9]。

在 Baek 等人所提出的 UDVSP 协议中没有定义不可传递性，我们认为既然 UDVSP 在某些情况下要作为 UDVS 的代替者，所以它还应该满足 UDVS 中的不可传递性[8]：即指定验证者无法提供一个证据证明签名者确实签署了该签名。更确切地说，指定验证者与原签名者所提供的零知识证明在计算上是不可区分的。

3　Baek 等人方案的安全缺陷

关于 Baek 等人的原方案请参考文献[9]。 在该方案中，签名持有者 Alice 在和指定验证者 Bob 进行 UDVSP 中的交互式协议：首先，Alice 和 Bob 计算 v_1 和 v_2，然后 Alice 要产生一个随机数 s，计算并传送 $\omega = v_2^s$ 给 Bob，Bob 接到 ω 之后，产生一个随机数 c，然后送给 Alice，Alice 得到 c 后计算 $t = s + cz \bmod q$，把 t 传给 Bob，最后由 Bob 来验证 v_2^t 与 ωv_1^c 是否相等，若相等则 Alice 持有的签名有效，否则无效。在这个过程中，有一个严重的安全问题，需要 Bob 生成的参数 c 是随机的。如果 Bob 别有用心，他可以通过某个特定的单向杂凑函数 $H^*()$ 来生成 $c = H^*(v_1, v_2, \omega, m, g, y)$，由于单向杂凑函数具有伪随机性，Alice 在收到 c 后不会辨别出其是否具有随机性。当 Alice 转化 c 得到 t 并传给 Bob 后，根据 Fiat-Shamir 的模型 (具体请参看文献[10])，可以将一个交互式方案转化成非交互式的数字签名，则 Alice 就可以向第三者证明 Bob 持有的签名是正确的。此时，该 UDVSP 就不具有 UDVS 所要求的不可传递性。

4　广义指定验证者签名证明协议

本节给出一个新的安全的广义指定验证者签名证明协议，其基本思想是 Bit 承诺方案来保证 c 的随机性。系统中有 3 方：签名者，签名持有者，指定验证者。在产生系统公钥/私钥对后，签名者对消息进行签名得到初始签名，然后将初始签名转化后送给签名持有者(在安全信道下传送)，签名持有者在得到初始签名后，用一个随机数将初始签名转化。接下来签名持有者通过一个交互式协议来向指定验证者证明他持有的签名是有效的。

4.1 基于 BLS 签名的广义指定验证者签名证明协议

本节将利用 BLS 签名[15]给出一个新的广义指定验证者签名证明协议，它由下面 5 个多项式时间算法和一个协议组成：

SigKeyGen：给定安全参数 k，计算 $(q, g, e, G_1, G_2) \leftarrow \mathrm{PramGen}(k)$；选择随机数 $x \in {}_R Z_q^*$，计算 $y = g^x$；令 $H: \{0,1\}^* \to G_1$ 与 $H^*: \{0,1\}^* \to Z_q$ 是两个安全的单向杂凑函数；输出 $pk = (k, q, g, e, G_1, G_2, H, H^*, y)$ 和 $sk = x$。

Sign：计算 $\sigma = H(m)^x$，其中 $m \in \{0,1\}^*$，输出 σ。

Verify：比较 $e(\sigma, g)$ 是否等于 $e(H(m), y)$，若相等则输出 1，若不相等则输出 0。

Tranform：选择随机数 $z \in {}_R Z_q^*$，计算 $\boldsymbol{\sigma}^z = H(m)^{xz}$。输出 $\tilde{\sigma} = \sigma^z$ 和 $s\tilde{k} = z$。

IVerify$[v(s\tilde{k}) \leftrightarrow p](pk, \tilde{\sigma}, m)$：P 和 V 首先计算 $v_1 = e(\tilde{\sigma}, g)$，$v_2 = e(H(m), y)$，然后执行下面的交互式协议(见图 1)：

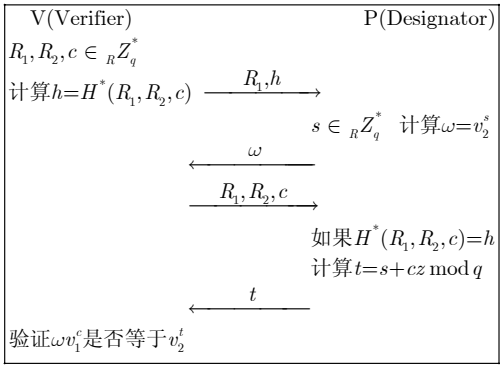

图 1　IVerify 协议

(1)承诺生成：V 选择随机数 $R_1, R_2, c \in {}_R Z_q^*$，计算 $h = H^*(R_1, R_2, c)$，然后将 (R_1, h) 给 P。

(2) P 选择随机数 $s \in {}_R Z_q^*$，计算 $\omega = v_2^s$，然后将 ω 传给 V。

(3)承诺兑现：V 将 (R_1, R_2, c) 传给 P。

(4) P 计算 $H^*(R_1, R_2, c)$，并与 h 比较，若相等则 V 的承诺合法，协议继续执行，若不相等，则 V 的承诺不合法，协议中止。

(5) P 计算 $t = s + cz \bmod q$，然后将 t 传给 V。

(6) V 比较 ωv_1^c 是否等于 v_2^t，若相等则输出 1，签名有效；若不相等则输出 0，签名无效。

4.2 安全性分析

下面证明本文的系统满足 UDVSP 所定义的安全属性。

定理 1　在随机预言模型下，假设群 G_1 中的OMDL问题是困难的，那么本文所提出UDVSP系统在Type-1攻击下是安全的。

定理 2　在随机预言模型下，假设群 G_1 中的 CDH 问题是困难的，那么本文所提出 UDVSP 系统在 Type-2 攻击下是安全的。

定理 1，定理 2 证明与文献[9]中定理的证明类似，故省略。本节重点证明定理 3，即不可传递性。

定理 3　本文的方案满足不可传递性。

证明　在我们的协议中，V 在 P 发送 ω 前必须选择 c，

因此 c 的选择与 ω 是无关的。而且由于 Bit 承诺协议的性质，在 P 发送 ω 给 V 后， V 无法改变 c 的值。这样就保证了 c 的随机性，这就使得 UDVSP 中的协议确实是一个交互式的协议，从而就实现了协议的不可传递性。更精确地说， V 可以以不可区分的方式来产生零知识证明协议，即下面两个五元组在计算上是不可区分的。

$$(\omega, R_1, R_2, c, t): \begin{cases} R_1, R_2, c \in Z_q^* \\ h = (R_1, R_2, c) \\ \omega = v_2^s \\ t = s + cz \end{cases}$$

$$(\omega, R_1, R_2, c, t): \begin{cases} R_1, R_2, c \in Z_q^* \\ h = (R_1, R_2, c) \\ t \in Z_q^* \\ \omega = v_2^t / v_1^c \end{cases}$$

也就是说，当 V 提供 (ω, c, t) 给第三方时，第三方无法相信 P 拥有一个正确的签名，因为 V 拥有和 P 一样的能力来产生 (ω, c, t) 使得 $v_2^t = \omega v_1^c$ 。 从而保证了不可传递性。

5 结束语

UDVS 在匿名信用证书系统中有着重要的作用，然而它需要签名持有者与指定的验证者通过签名者的公钥体系来生成自己的公钥和私钥，这在指定验证者不合作的情况下是不现实的。Baek 等人提出了 UDVSP 的概念来解决这个问题。然而，本文指出 Baek 等人所提出的 UDVSP 不满足 UDVS 所有的不可传递性，从而在实际应用中无法完全代替 UDVS。我们利用承诺方案来解决这个问题并给出了一个高效的，安全的指定验证者签名证明协议。本文证明了该协议满足所定义的安全性质。

参 考 文 献

[1] Chaum D and Antwerpen H. Undeniable signatures. Crypto 1989, Springer-Verlag, 1990, LNCS 435: 212–216.

[2] Jakobsson M, Sako K, and Impagliazzo R. Designated verifier proofs and their applications. Cryptology-Eurocrypt 1996, Springer- Verlag, 1996, LNCS 1070: 143–154.

[3] Huang X, Susilo W, Mu Y, and Zhang F. Short (identity -based) strong designated verifier signature schemes. Information Security Practice and Experience (ISPEC 2006), Springer-Verlag, 2006, LNCS 3903: 214–225.

[4] Kurosawa K and Heng S. Relations among security notions for undeniable signature schemes. Security and cryptography for networks (SCN 2006), Springer-Verlag, 2006, LNCS 4116: 34–48.

[5] Kurosawa K and Takagi T. New approach for selectively convertible undeniable signature schemes. ASIACRYPT 2006, Springer-Verlag, 2006, LNCS 4284: 428–443.

[6] Monnerat J and Vaudenay S. Short 2-move undeniable signatures. VIETCRYPT 2006, Springer-Verlag, 2006, LNCS 4341: 19–36.

[7] Laguillaumie F, Libert B, and Quisquater J. Universal designated verifier signatures without random oracles or non-black box assumptions. Security and Cryptography for Networks (SCN 2006), Springer-Verlag, 2006, LNCS 4116: 63–77.

[8] Steinfeld R, Bull L, Wang H, and Pieprzyk J. Universal designated-verifier signatures. Cryptology Asiacrypt 2003, Springer-Verlag, 2003, LNCS 2894: 523–542.

[9] Baek J, Safavi-Naini R, and Susilo. Universal designated verifier signature proof (or How to efficiently prove knowledge of a signature). Cryptology-Asiacrypt 2005, Springer-Verlag, 2005, LNCS 3788: 644–661.

[10] Fiat A and Shamir A. How to prove yourself: Practical solutions of identification and signature problems. Cryptology-Crypto 1986, Springer-Verlag, 1986, LNCS 263: 186–194.

[11] Schneier B. Applied Cryptography-Protocols, Algorithms, and Source Code in C. John Wiley and Sons inc., Part I, Chapter 4, 1996.

[12] Boneh D and Franklin M. Identity-based encryption from the weil pairing. Cryptology-Crypto 2001, Springer-Verlag, 2001, LNCS 2139: 213–229.

[13] Bellare M, Namprempre C, Pointcheval D, and Semanko M. The power RSA inversion oracles and the security of chaum's RSA-based blind signature scheme. FC 2001, Springer-Verlag, 2002, LNCS 2339: 319–338.

[14] Goldwasser S, Micali S, and Rivest R. A digital signature scheme secure against adaptive chosen-message attack. *SIAM Journal on Computing*, 1988, 17(2): 281–308.

[15] Boneh D, Lynn B, and Shacham H. Short Signatures from the Weil Pairing. Advances in Asiacrypt 2001, Springer-Verlag, 2001, LNCS 2248: 566–582.

陈国敏： 男，1986 年生，本科生，研究兴趣为公钥密码学.

陈晓峰： 男，1976 年生，副教授，研究方向为公钥密码学及其应用.