Deniable Authentication vs. Strong Designated Verifier Signature

LI Yong, LIU Yun

Key Laboratory of Communication & Information Systems, Beijing Jiaotong University, Beijing, China

e-mail: *liyong@bjtu.edu.cn, liuyun@bjtu.edu.cn*

Abstract: Deniable authentication (DA for short) and designated verifier signature (DVS) both adapt for privacy protecting scenarios. For exploring the internal relationship of DA and DVS, the concrete mutual transformation between DA and strong DVS (SDVS) was presented, including ID-based DA being transformed into SDVS, and SDVS into DA. The correctness and security of the newly invert schemes are proved. New method to construct SDVS scheme was also proposed, i.e., building SDVS from transformed DA protocol. And the transformation method bridges the gap between DA and SDVS.

Keywords: cryptography; digital signature; designated verifier signature; authentication; deniable authentication

可否认认证与强指定验证者签名

李勇，刘云

北京交通大学通信与信息系统北京市重点实验室，北京，中国，100044

e-mail: liyong@bjtu.edu.cn, liuyun@bjtu.edu.cn

【摘　要】可否认认证(DA)协议和指定验证者签名(DVS)适用于具有隐私保护需求的认证应用。本文通过研究 DA 协议和 DVS 间的内在联系，给出具体的 DA 协议与强指定验证者签名（SDVS）相互转换构造的方法，包括：基于身份的 DA 协议转换为基于身份的 SDVS 方案、SDVS 方案转换为 DA 协议，并证明了转换后对应协议的正确性和安全性。本文同时给出构造 SDVS 的新方法，即从可否认认证协议转换构造 SDVS 的方法。通过 DA 与 SDVS 间的相互转换，架起了 DA 协议和 SDVS 之间的桥梁。

【关键词】密码学；数字签名；指定验证者签名；认证；可否认认证

1 引言

传统的认证协议允许发送方通过不安全通信信道传送消息给接收方，向接收方证实消息确实源自发送方而且消息没有被敌手篡改（数据起源认证或消息认证）；也可以提供关于某实体身份的保证（实体认证）。通过这类协议可建立起发送方到接收方的认证链路，可以有效地对付假冒攻击。但是直接应用传统的认证机制并不能满足一些实际应用的需要。比如，电子选举系统中的胁迫投票问题（coercion）：第三方胁迫投票人必须投某候选人的票。投票人 B 希望自己向计票机构投出选票（选候选人 A）后，计票机构可以认证此选票（候选人 A）来自投票人 B，但是计票机构不能向第三方证明此选票来自 B。假如 B 可以对投过的选票否认（相对计票机构之外的第三方），则可以解决第三方胁迫投票问题。满足上述需求的协议就是一种可否认认证（Deniable Authentication，简记 DA）协议[1]。与传统的认证协议相比，可否认认证协议有两个特征：（1）可以让意定的接收者鉴别给定消息的来源。（2）意定接收者不能向任意第三方证明给定消息的来源（除发送方和接收方外的第三方不能识别消息来源）。因此，可否认性属于一类隐私保护属性，因为协议参与方可以否认参与过协议执行。

指定验证者签名（Designated Verifier Signature，简记 DVS）的思想源于 1996 年由 Jakobsson 等人在欧密会上提出的指定验证者证明[1]。其主要特征是签名者 S 可以向指定的签名接收者（即指定验证者）V 证实他签署了一个声明，同时，V 不能向另一方证实签名的有效性，因为 V 具有模拟 S 签名的能力。这样就保证了签名证实（或否认）的不可转移性

资助信息：国家高技术研究发展计划(863 计划)项目(2009AA01Z423)北京交通大学科技基金项目(2007XM006)，北京交通大学红果园“双百”人才培育计划资助.

978-1-935068-06-8

（non-transferability），即限制验证者使其不能把签名任意提供给第三方。

DA 协议和 DVS 在概念和应用场景上有些类似，那么这两类协议在方案构造上是否存在一些内在的系呢？就作者所知的公开文献中，还没有专门研究 DA 协议和 DVS 之间关系的文献。因此，本文通过对 DA 协议和 DVS 具体方案的构造分析，考察 DA 协议和 DVS 间的转换关系，尝试在两类协议之间架起一座桥梁。

本文的组织如下：第 2 节介绍了 DA 协议与指定验证者签名相关概念；第 3 节研究 DA 协议和强指定验证者签名间的构造与相互转换；第 4 节对本文进行了总结。

2 相关概念

2.1 可否认认证

可否认认证（DA）的思想是由 Dolev、Dwork 和 Naor 首次提出的[2]。1998 年，Dwork 等学者对 DA 进一步形式化[3]，基于并发零知识证明提出一个 DA 协议，其缺点是协议需要定时限制（Timing），认证步骤中的知识证明有时间延迟。随后，许多学者陆续提出一些 DA 方案，如基于因子分解的 DA 协议[4,5]、对 2 轮定时 DA 协议的改进方案[6]、基于身份的 DA 协议[7]等。

定义 1 非形式的，可否认认证协议可以向验证方 V 证实 P 对消息 m 进行了认证，但是不允许 V 向第三方证实这个事实（P 认证过消息 m）。

可否认认证协议的基本安全需求如下：

正确性：对任何消息 m，如果认证者 P 和验证者 V 执行的协议是为了认证消息 m，那么，验证者 V 接受。

可否认性(Deniability)：假定认证者 P 将认证消息 m，则对每一个攻击者 A，都存在一个多项式时间的模拟算法 Sim，模拟算法的输出与协议实际执行的输出是不可区分的。

2.2 指定验证者签名

令 S 表示签名者，D 表示指定验证者；D 的公钥和私钥分别记为 PK_D 和 SK_D。指定验证者模拟签名算法记为 $Simul_{PKS,PKD,SKD}$。下面给出 DVS 定义：

定义 2 令 M 为消息空间，一个指定验证者签名（DVS）方案由以下算法组成：

- 创建 Setup(k)：是一个概率算法，输入安全参数 k，输出公共参数 params；
- 密钥生成 KeyGen (params)：是一个概率算法，输入公共参数，输出私钥/公钥对(SK,PK)；
- 签名算法 $Sign_{SKS,PKD}(m)$：输入签名者私钥、指定验证者公钥、消息 $m \in M$，输出签名 σ；
- 验证算法 $Verify_{PKS,PKD}(m,\sigma)$：是一个确定算法，输入签名者公钥 PK_S、指定验证者 D 的公钥 PK_D、消息 $m \in M$、签名 σ，输出 accept 或 reject。

若 $Verify_{PKS,PKD}(m,\sigma)$=accept，则称对消息 m 的签名 σ 是有效的。一个 DVS 方案是正确的，即对 KeyGen 输出的所有(SK_S,PK_S)和(SK_D,PK_D)，对所有的 $m \in M$，有 $Verify_{PKS,PKD}(m,Sign_{SKS,PKD}(m))$=accept。

一个 DVS 是安全的，如果满足下面的基本属性：

不可伪造性：非形式的，不可伪造性指协议任何一方不能伪造签名者对消息 m 的签名。

不可转移性(Non-transferability)：非形式的，不可转移性是指给定 D 接受的消息--签名对(m,σ)，除签名者和指定验证者外，要确定 σ 是 S 的签名还是 D 模拟的签名是计算不可行的。

注 1：在 DVS 中，不可转移性通常由指定验证者执行的模拟算法来保证，即，模拟算法 $Simul_{PKS,PKD,SKD}(m)$：输入签名者公钥、指定验证者公钥、指定验证者 D 的私钥、消息 $m \in M$，输出签名 σ。

注 2：若一个 DVS 验证算法需要输入指定验证者的私钥 SK_D，否则无法进行验证，则称其为强指定验证者签名（Strong DVS，简记 SDVS）。强指定验证者签名必然是指定验证者签名，反之未必[2]。

3 DA 协议与 SDVS 间的构造及转换

本节首先归纳了目前文献中 DA 协议的主要构造方法，然后研究了两个具体的方案：基于身份的 DA 协议[7]和 SDVS[8]，指出每个方案都可以转换成相对的协议（DA 转换为 SDVS 和 SDVS 转换为 DA）。

3.1 DA 协议构造方法

目前文献中一些 DA 协议的具体构造方法可以划分为基于对称密码体制和基于非对称密码体制的两大类方法：在对称密码体制框架下，DA 协议可以使用消息认证码（MAC）实现。一般方法是：发送方和接收方能够各自计算出共享秘密，共享秘密作为 MAC 的密钥。因为双方都可以计算共享秘密，所以任一方都可以否认参与过协议执行。

在非对称密码体制下的 DA 协议，发送方和接收方不共享任何秘密信息，认证需借助于发送方相关公钥

完成。基本构造思想是：发送方用接收方的公钥构造会话密钥 k，用 k 作消息认证码 MAC 的密钥；接收方用自己的私钥从收到的信息中恢复出会话密钥，计算消息的 MAC 值。比较计算出的 MAC 值和发送方传来的 MAC 值，若二者相等，接收方确信消息来自发送方。因为接收方具有和发送方同等的计算会话密钥和 MAC 值的能力，所以第三方无法区分消息是经发送方认证的还是接收方模拟的认证消息，从而保证了可否认性。

3.2 基于身份的 DA 协议转换为 SDVS

曹天杰等学者在文献[7]中构造了一个基于身份的 DA 协议（简称 ID-DA），该协议可以平滑地转化为基于身份的 SDVS 方案，具体转化步骤如下（假定通信双方为 A 和 B，e 为双线性映射）：

- *Setup*：延用 ID-DA 中的 Setup 算法，得到系统主密钥 $s \in Z_q^*$，输出公开参数 $params = (q, G_1, G_2, e, n, P, P_{pub}, H_1, H_2, H_3, E)$。其中 $E: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ 是对称加密算法。
- *KeyGen*：使用 ID-DA 中的 Extract 算法，给定身份 $ID \in \{0,1\}^*$，私钥生成中心 PKG 计算 $Q_{ID} = H_1(ID)$，输出私钥 $S_{ID} = sQ_{ID}$。
- *Sign*：修改 ID-DA 中的 Authenticate 算法，签名者计算

$$Q_{IDB} = H_1(ID_B),$$
$$Y = e(TP_{pub} + S_{IDA}, TP + Q_{IDB}),$$
$$K = H_2(Y, ID_A), MAC = H_3(K, m),$$
$$c = E(K, m).$$

其中 $T \in Z_q^*$ 是时间戳，得到签名 (T, MAC, c)。

- *Verify*：收到签名者 A 的签名 (T, MAC, c) 后，验证者 B 计算

$$Y^* = e(TP + Q_{IDA}, TP_{pub} + S_{IDB}),$$
$$K^* = H_2(Y^*, ID_A), m^* = E(K^*, c),$$
$$MAC^* = H_3(K^*, m^*).$$

若 $MAC^* = MAC$ 且时间戳 T 有效，验证者输出 Accept，否则 Reject。

指定验证者模拟签名算法 *Simulation*：由 *Verify* 算法，验证者可以模拟签名者的签名 (T, MAC, c)。即有，

$$Y = e(TP + Q_{IDA}, TP_{pub} + S_{IDB}),$$
$$MAC = H_3(H_2(Y, ID_A), m),$$
$$c = E(H_2(Y, ID_A), m).$$

下面证明转化后的 ID-SDVS 的安全性：

定理 1：按上述方法得到的强指定验证者签名是正确的 $(correctness)$。

证明：若 (T, MAC, c) 由签名者按上述方法生成，则有

$$\begin{aligned} Y^* &= e(TP + Q_{IDA}, TP_{pub} + S_{IDB}) \\ &= e(TP + Q_{IDA}, s(TP + Q_{IDB})) \\ &= e(s(TP + Q_{IDA}), TP + Q_{IDB}) \\ &= e(TP_{pub} + S_{IDA}, TP + Q_{IDB}) \\ &= Y \end{aligned}$$
$$K^* = H_2(Y^*, ID_A) = H_2(Y, ID_A) = K,$$
$$MAC^* = H_3(K^*, m^*) = H_3(K, m) = MAC.$$

因此，按照协议步骤得到的签名总可以通过 *Verify* 算法验证，即

$$Pr[Verify(S_{IDB}, m, Sign(ID_B, S_{IDA}, m)) = accept] = 1.$$

定理 2：按上述方法得到的强指定验证者签名满足不可转移性 $(non-transferability)$。

证明：由模拟算法 *Simulation*，验证者可以模拟签名者的签名，因而验证者无法让第三方相信 (T, MAC, c) 是签名者对 m 的签名，不可转移性满足。

通过上述方案转换，我们得到构造（基于身份的）SDVS 的新模式，即由可否认认证协议转化构造 SDVS 的一种方法。具体的说，通过签名者、验证者双方用各自私钥计算的秘密信息 (Y)，得到共享密钥 K。通过 K，签名者计算对消息 m 的 MAC 值和密文 c，验证者从密文 c 中恢复出消息，进而计算出 MAC 值并与签名者发送的 MAC 值比较。签名和验证算法可以表示如下：

- 签名生成：

$$Sign(PK_B, SK_A, m) = \begin{cases} Y = f(SK_A, PK_B); \\ K = H(Y, PK_A); \\ MAC = H(K, m); \\ c = Encrypt(K, m). \end{cases}$$

其中，SK_A 是签名者 A 的私钥，PK_B 是验证者 B 的公钥、*Encrypt* 是加密方案、$f()$ 是一单向置换。得到对消息 m 的签名 $\sigma = (MAC, c)$。

978-1-935068-06-8 © 2009 SciRes.

■ 签名验证：

$$Verify(SK_B, m, \sigma) = \begin{cases} Y^* = g(SK_B, PK_A); \\ K^* = H(Y^*, PK_A); \\ m = Decrypt(c, K^*); \\ MAC^* = H(K^*, m); \\ MAC^* \stackrel{?}{=} MAC. \end{cases}$$

其中，$g()$ 是满足

$$g(SK_B, PK_A) = f(SK_A, PK_B)$$

的单向置换、SK_B 是验证者的私钥，PK_A 是签名者公钥、*Decrypt* 是解密算法。验证结果输出签名“真”或⊥。

3.3 SDVS 转换为 DA

在 CISC 2005 上，Tso 等学者提出一个用单向两方密钥协商协议和对称密钥密码系统构造 SDVS 的基本方法[8]：

- 签名：
  - 令 $\mathbb{G}$ 是一个乘法群，生成元为 g，Alice 随机选择 $r \in \mathbb{G}$，计算 $R = g^r$。
  - 对预定义的单向两方密钥协商协议 *KeyAgr* 输入 r、Alice 的私钥、Bob 的公钥，*KeyAgr* 为 Alice 输出会话密钥 K_{AB}。
  - 预定义的对称加密算法 *Enc* 使用会话密钥 K_{AB} 对消息 m 加密，*Enc* 输出密文 $C \leftarrow Enc_{K_{AB}}(m)$。
  - 消息 m 的 SDVS 是 $\sigma \leftarrow (R, C)$。
- 验证：
  - 输入 R、*Bob* 的私钥和 Alice 的公钥到 *KeyAgr*，*KeyAgr* 为 *Bob* 输出会话密钥 K_{BA}。
  - 输入 K_{BA} 和消息 m 到加密算法 *Enc*，*Enc* 输出密文 $\widetilde{C} \leftarrow Enc_{K_{BA}}(m)$。
  - σ 是有效签名当且仅当 $\widetilde{C} = C$。

由此方法，Tso 等学者提出了低通信、低计算代价的 SDVS 方案（简称 TOO05 方案）[8]，方案基于 Diffie-Hellman 密钥分配和双离散对数，安全性可以归约到 CDH 和 DDH 问题。

TOO05 方案简述如下：

p 是一个大素数，使得 $q = (p-1)/2$ 也是素数，$g \in Z_p^*$ 是阶为 q 的元素，h 是 Z_p^* 生成元，计算以 g 和 h 为基底的离散对数是困难的。

- 系统参数生成 $(SysGen)$：输入 1^K，可信机构(TA)调用系统参数生成算法 *SysGen* 输出如下公共参数：
  - 大素数 p，使得 $q = (p-1)/2$ 也是素数，在 Z_p^* 上计算离散对数是困难的；
  - $g \in Z_p^*$ 是阶为 q 的元素，计算以 g 为基底的离散对数是困难的。
  - $H: \{0,1\}^* \to Z_p^*$ 是一个抗碰撞哈希函数。
- 密钥生成 $(KeyGen)$：TA 生成各方公/私钥对。对实体 Alice 和 Bob，随机选择 $\{a, b\}_R Z_q^* \times Z_q^*$，计算

  $V_a \leftarrow g^a \bmod p, V_b \leftarrow g^b \bmod p$。

  Alice 和 Bob 的私/公钥对分别是 (a, V_a) 和 (b, V_b)。
- 签名生成 $(Sign)$：Alice 对消息 $m \in \{0,1\}^*$ 签名，指定 Bob 为验证者。Alice 执行以下步骤：给定 Alice 私钥 a、Bob 的公钥 V_b，计算 $V_b^a \bmod p$；然后计算 $H(m)$ 和 $H(m)^{V_b^a} \bmod p$；得到签名 $\sigma \leftarrow H(m)^{V_b^a}$。
- 验证 $(Veri)$：Bob 执行 *Veri* 算法。给定 Bob 的私钥 b 和 Alice 的公钥 V_a，计算 $V_a^b \bmod p$。给定消息 m，计算 $H(m)$ 和 $\widetilde{\sigma} \leftarrow H(m)^{V_a^b} \bmod p$。当且仅当 $\sigma = \widetilde{\sigma}$，接受 σ 为有效签名。

定理 3（不可伪造性）若存在算法 A 可以

$$(\tau, q_h, q_s, \varepsilon)$$

攻破 SDVS 方案（在自适应选择消息攻击下方案是存在伪造的），则可以构造算法 B 能 (τ', ε') 破解 Z_p^* 上的 CDH 问题，其中

$$\tau' \le \tau + (q_h + q_s)\tau_{Exp} + (q_h - q_s)\tau_{MC} + 1\tau_{Inv},$$

$$\varepsilon' = 1/q_s \cdot (1 - 1/(q_s + 1))^{(q_s+1)} \varepsilon$$

其中，τ_{Exp}、τ_{MC} 和 τ_{Inv} 分别表示 Z_p^* 上指数运算、乘运算和逆运算的时间消耗。

类似的，上述 SDVS 方案也可以转化为 DA 协议：系统参数生成、密钥生成算法保持不变，发送方用接收方公钥和自己的私钥计算共享密钥

$$V_b^a \bmod p,$$

然后用共享密钥对 $H(m)$ 加密；接收方收到认证信息后，首先用发送方公钥和自己的私钥计算出共享密钥

$$V_a^b \bmod p,$$

然后用共享密钥对 $H(m)$ 加密；比较两个加密结果，若相同，则可以确信是发送方对消息 m 的认证。否则，接收方拒绝该认证。

可以看到，3.2 节中由 DA 协议构造 SDVS 的基本模式和 3.3 节由 SDVS 构造 DA 协议的基本思想是一致的，实质上是利用单向两方密钥协商计算共享秘密（会话密钥）、进而用对称密码算法和共享秘密对消息（或消息的哈希值）加密。单向两方密钥协商协议 *KeyAgr* 对应 3.2 节基本模式中的单向置换 $f()$ 和 $g()$。

4 结束语

从考察 DA 协议与 DVS 间的内在联系入手，本文给出了具体的 DA 协议与 SDVS 相互转换构造的方法：基于身份的 DA 协议[7]转换为基于身份的 SDVS 方案、 SDVS[8]转换为 DA 协议，并证明了转化后对应协议的正确性和安全性。本文同时给出构造强指定验证者签名的新方法，即从可否认证协议转换构造 SDVS 的方法。利用 3.2 节给出的 DA 转换构造 SDVS 和 3.3 节给出的 SDVS 转换构造 DA 的基本方法，架起了可否认证协议和强指定验证者签名之间的桥梁。

5 致谢

感谢审稿专家提出的修改意见。

References (参考文献)

[1] M. Jakobsson, K. Sako, R. Impagliazzo, Designated Verifier Proofs and Their Applications, In: Ueli Maurer ed. Proceedings of the Advances in Cryptology-EUROCRYPT'96 [C], Berlin: Springer-Verlag, 1996. LNCS 1070, 143~154.

[2] D. Dolev, C. Dwork, M. Naor. Non-Malleable Cryptography. In: ACM Symposium on Theory of Computing [C], ACM, 1991. 542~552.

[3] C. Dwork, M. Naor, and A. Sahai. Concurrent Zero-Knowledge. In: Proc. of 30th Symposium on Theory of Computing (STOC) [C], ACM, 1998. 409~418.

[4] Y. Aumann, M. Rabin. Efficient deniable authentication of long messages, In: Int. Conf. on Theoretical Computer Science in Honor of Professor Manuel Blum's 60th birthday [EB/OL]. http:// ww.cs.cityu.edu.hk/dept/video.html. 1998.

[5] X. Deng, C.H. Lee, H. Zhu. Deniable authentication protocols. IEE Proceedings Computers and Digital Techniques [C], 2001. 148(2): 101~104.

[6] Y. Zhao, C.H. Lee, Y. Zhao, H. Zhu. Some Observations on Zap and Its Applications. In: M. Jakobsson et al. eds., ACNS 2004 [C], Berlin: Springer-Verlag, 2004. LNCS 3089, 180~193.

[7] Tianjie Cao, Dongdai Lin, Rui Xue. An Efficient ID-Based Deniable Authentication Protocol from Pairings. In: Proc. of 19th International Conference on Advanced Information Networking and Applications (AINA'05) [C], IEEE, 2005. Vol. 1: 388~391.

[8] Raylin Tso, Takeshi Okamoto, Eiji Okamoto. Practical Strong Designated Verifier Signature Schemes Based on Double Discrete Logarithms. In: SKLOIS Conference on Information Security and Cryptology [C], Berlin: Springer-Verlag, 2005. LNCS 3822, 113~127.