可验证秘密分享及其应用

张福泰[1], 赵福祥[2], 王育民[2]
(1. 南京师范大学数学与计算机科学学院, 江苏南京, 210097; 2. 西安电子科技大学 ISN 国家重点实验室, 陕西西安, 710071)

摘 要: 可验证秘密分享(VSS)是设计安全的密码协议的一个基本工具, 自从其概念于 1985 年被提出后, 受到了密码学和信息安全界的普遍关注, 到现在为止已经取得了大量的研究成果. 本文全面总结和评述了该领域已经取得的重要成果, 并探讨了该领域研究的发展趋势, 指出了几个值得重视的研究方向.

关键词: 秘密分享; 可验证秘密分享 (VSS); 多方安全计算; 门限密码学; 电子商务
中图分类号: TN918.4 文献标识码: A 文章编号: 0372-2112 (2002) 10-1519-07

Verifiable Secret Sharing and Its Applications

ZHANG Fu-tai[1], ZHAO Fu-xiang[2], WANG Yu-min[2]
(1. *School of Mathematics and Computer Science, Nanjing Normal University, Nanjing, Jiangsu, 210097, China;*
2. *Key Lab. On ISN, Xidian University, Xi'an, Shaanxi, 710071, China*)

Abstract: Verifiable secret sharing (VSS for short) is a fundamental tool for the design of secure cryptographic protocols. Its notion was proposed in 1985. From then on, it has been drawing the attentions of many researchers in the fields of cryptography and information security, and a great deal of achievement has been made in the field of VSS and its applications. In this paper, we analyze and survey in detail the main results available in literature in the field. We also analyze the development trend of the researches in the field and point out some research directions that deserve taking into account.

Key words: secret sharing; verifiable secret sharing; secure multiparty computation; threshold cryptography; electronic commerce

1 引言

秘密分享是信息安全和数据保密中的重要手段, 它在重要信息和秘密数据的安全保存、传输及合法利用中起着非常关键的作用. 秘密分享的概念最早是由 Shamir[1] 和 Blakley[2] 提出的. 秘密分享由两个算法——秘密份额的分配算法和秘密的恢复算法构成. 在执行秘密份额的分配算法时, 分发者 (Dealer) 将秘密 s 分割成若干个份额(share, 或小块 piece, 或影子 shadow) 在一组参与者 $P=\{P_1, P_2, \cdots, P_n\}$ 中进行分配, 使得每一个参与者都得到关于该秘密的一个秘密份额; 秘密的恢复算法保证只有 P 的一些特定的子集(称为合格子集)[3-5] 才能有效地恢复 s, 而 P 的其它子集不能有效地恢复秘密 s, 甚至得不到关于 s 的任何有用信息.

通常的秘密分享方案, 包括动态秘密分享方案在内, 在安全性方面, 都附加了秘密分发者和分享者是诚实的假设. 然而, 这样的假设在现实生活中往往是不切实际的. Chor 等人于 1985 年提出了可验证秘密分享(Verifiable Secret Sharing, 简记为 VSS) 的概念[6], 用以解决分发者欺骗的问题. 可验证秘密分享是在秘密分享的基础上增加了一个验证算法而形成的. 在已经提出的诸多 VSS 方案中, 也提供了防止分享者欺骗的功能[7-9]. 由于可防止分享者欺骗的可验证秘密分享方案有良好的安全性质, 它在诸如多方安全计算[9-12] 等方面有着广泛的应用. 自从可验证秘密分享的概念提出以来, 不少学者对其概念的定义进行了研究. 除了其创始人的工作外, 主要的还有文献[13] 和[14].

在文献[13] 中, Gennaro 和 Micali 对文[6] 中给出的 VSS 的定义进行了加强, 给 VSS 增加了归约性性质(Reducibility), 并提出了第一个满足这样的定义的 VSS 协议. 在其定义中, 他们是把 VSS 作为安全计算来对待的.

在文献[14] 中, Gennaro 给出了 VSS 的一个新的定义. 其新意在于给 VSS 增加了安全协议的组合性质(composition property), 即要求安全的 VSS 协议在被用作大的协议中的子协议时仍然可被证明是安全的. 这一性质是以前的定义所没有要求的. 这一改进使得满足新的定义的安全的 VSS 协议可以被放心的应用于各种大的协议中而不必担心其安全性会降低.

到现在, 可验证秘密分享领域的研究已经取得了不少成果[7-73], 下面将对这些成果做较为细致的总结与评述. 期望对相关的科研人员能够提供一点帮助.

收稿日期: 2001-07-02; 修回日期: 2001-12-19
基金项目: 国家自然科学基金(No. 60073052); 教育部博士点基金(No. 2000070101)

2 几个主要的 VSS 方案

2.1 交互式的 VSS 方案

VSS 方案从其验证算法是否需要参与者之间或参与者与分发者之间进行交互可分为两类,即交互式的和非交互式的. 早期的 *VSS* 方案都是交互式的[6, 9, 10, 15],因而其效率都不够理想. 文献[6]以 1 比特的秘密为例给出了一个交互式的 VSS 协议. 该协议是以大整数分解的困难性和不经意传输为基础的. Goldreich, Micali 和 Wigderson 在文献[16]中利用比特承诺和零知识证明技术提出了如下的一个 VSS 协议: 在分发阶段,对秘密 $s \in K$(有限域),分发者 D 按照 Shamir 秘密分享方案中的方法计算给各参与者的份额 $s_1, s_2, \cdots, s_n$. 接着计算并向全体参与者广播对 $s_1, s_2, \cdots, s_n$ 的承诺 $C_1, C_2, \cdots, C_n$. 之后, D 以零知识方式向所有参与者证明这些承诺包含了对应于某一秘密的的正确的份额. 如果他的证明被参与者接受,他再把 s_j 及打开 C_j 的信息秘密地发给参与者 P_j, $j = 1, 2, \cdots, n$; 在恢复阶段,每一 P_j 广播他的秘密份额 s_j 及打开 C_j 的信息,利用 t(门限值)个正确的份额(承诺可以被成功打开的份额),就可用拉格郎日多项式插值法恢复出秘密 s. 这一协议可抵抗 $t-1 < n/2$ 个恶意的参与者,而且恶意参与者的不端行为只能是在恢复阶段拒绝参与,但他们无法阻止诚实的参与者恢复秘密. 该协议具有很好的安全性和可靠性,可应用于交互式的多方安全协议中.

2.2 非交互式的 VSS 方案

Feldman 于 1987 年首先提出了不需可信机构的非交互式 (t, n) 门限 VSS 协议[7](以后简称为 Feldman VSS). 该协议是基于 Shamir 的门限体制和计算离散对数的困难性假设的. 由于其效率较高,在门限密码学[17]、分布式密钥生成[18],多方安全计算[11, 12]等诸多方面得到了广泛的应用. 该协议能够抵抗包括分发者在内的 $(n-1)/2$ 个恶意参与者的合谋攻击.

在文献[8]中, Pedersen 首先给出了一个具有同态性质的安全的承诺方案,之后基于拉格郎日多项式插值法,提出了第一个信息论安全(无条件安全)的非交互式可验证秘密分享方案(以后简称为 Pedersen VSS). 这一方案的信息速率为 1/2,与文[7]中的方案一样具有较高的效率,同时在安全性方面具有下述三条重要性质:

(1) 如果分发者在协议中始终是诚实的,那么所有诚实的参与者持有的份额能够以拉格郎日多项式插值法确定出惟一的一个 $t-1$ 次多项式(这里的 t 是门限值). 特别地,这些份额中的任何 t 个足以有效地恢复秘密.

(2) 方案中提供了在秘密恢复阶段用于检验每一份额的正确性的信息,因而,在即使有恶意参与者存在的情况下,份额集合的任何包含 t 个正确份额的子集都可用来正确地恢复出秘密.

(3) 至多能与 $t-1$ 个分享者合谋的攻击者,在协议中所得到的信息是独立于被分享的秘密的,因此所分享的秘密是信息论安全的(无条件安全的).

Gennaro 等人在文献[19]中,基于一个高效的承诺方案提出了一个结构非常简单的 VSS 方案. 这一方案避免了以前的 VSS 方案中通常用来保证参与者正确行为的零知识证明过程,因而与以前的 VSS 方案相比,大大地提高了通信和计算效率. 该方案的运行过程大致如下:

分发者选两个随机的 $t-1$ 次多项式 $f(x)$, $r(x)$,并使 $f(x)$ 的常数项为要分享的秘密. 多项式 $r(x)$ 用于生成对分享者的份额进行承诺的随机串. 每一分享者 P_i 将收到他的份额 $f(i)$ 及与之对应的随机值 $r(i)$. 分享者通过广播 $C(f(i), r(i))$, $i = 1, 2, \cdots, n$, 对所有分享者的份额做出公开的承诺. 其中的 $C(x, r)$ 是一个承诺函数,如单向 hash 函数 $SHA\text{-}1(x, r)$. 承诺函数可用来对所有分享者的秘密份额的正确性进行检验. 在恢复秘密时,根据拉格郎日插值法,任何 t 个正确的秘密份额可惟一确定出秘密.

上面这三个方案是到目前为止最有实用价值的 VSS 方案,它们都具有很好的安全性. 但从历史上看,文[7]中的方案是第一个不需要可信机构的非交互式 VSS 方案,文[8]中的方案是第一个信息论安全的非交互式 VSS 方案,而且它们都要比文[19]中的方案要早,因而它们是目前应用得最多的 VSS 方案. 由于其效率很高,我们相信文献[19]中的方案将会受到越来越多的重视.

近期对门限 VSS 的研究,主要是设计具有特殊性质的 VSS 方案[62~67, 72]. Mu 等人[62]中提出了防失败的 VSS 方案; Pieprzyk 在文[63]中讨论了非线性的可验证秘密分享; Zhang 在文[64]中提出了免疫的 VSS 方案; 张福泰[65]讨论了在 VSS 中防止主动攻击的问题; Ayako 等人[72]提出了可变的 VSS 方案.

2.3 可公开验证的秘密分享方案

第一个 VSS 方案[5]的验证算法具有一个良好的性质,即任何人(不仅仅是分享者)都可以检验秘密份额分发过程的正确性. 但这一性质在后来的高效 VSS 方案中不复存在了,在这些高效的 VSS 方案[7, 8, 19]中,只有分享者本人才可以验证他自己收到的秘密份额的正确性. 这使 VSS 的应用在一定程度上受到了限制. 到 1996 年, Stadler 注意到了这一性质的重要性. 在文献[20]中, Stadler 把这一性质称为可公开验证性(public verifiability),并把具有这一性质的 VSS 方案称为是可公开验证的秘密分享(Publicly Verifiable Secret Sharing,简称 PVSS)方案. 他在这一文献中给出了 PVSS 的一个非形式化的模型,同时还给出了两个 PVSS 协议,其中的一个基于对离散对数的可验证加密,另一个基于对模复合数的 e 次根的可验证加密. 由于通信和计算代价都很大,这两个协议的效率都很低. Fujisaki 和 Okamoto[21]于 1998 年提出了一个效率相对较高的 PVSS 方案. 其方案的构造利用了几个高效的承诺方案,而安全性是依赖于改进的 RSA 假设的. Schoenmakers[22]对 Stadler 和 Fujisaki 等人的 PVSS 模型做了简单的改进. 在改进的模型中,要求每一分享者在恢复算法中不仅提供其秘密份额,而且要提供其秘密份额正确性的证明. 基于改进的模型, Schoenmakers[22]提出了一个构造简捷、安全性和效率比以前的 PVSS 方案更高的一个新的 PVSS 方案. 新方案的安全性所依赖的困难问题是离散对数问题和决策 Diffie-Hellman 问题,其困难性假设是所有基于离散对数的密码系统的共同基础,因而其要求是最低的.

到目前为止, 文献中所能见到的 PVSS 方案主要的就是上面列举的这几个. 从它们的安全性和性能方面的特点来看, 文[22] 中的方案要优于其它方案. 而文献[20], 由于是 PVSS 的概念和实现方面的开创性的工作, 受到了研究人员的普遍重视.

2.4　可验证多秘密分享方案

传统的秘密分享方案都是一次性的方案, 分享者所持有的份额只能使用一次. 在实际中, 有些场合需要在同一组分享者中分享多个秘密, 为此目的, 所使用的秘密分享方案应能够使分享者重复使用其秘密份额[23]. 这样的秘密分享方案被称为多秘密分享方案[24, 25, 26]. 第一个可验证多秘密分享(Verifrable Multi-Secret Sharing, 简称 VMSS) 方案是 Ham[27] 提出的. 在其方案中, 每一分享者持有一个由分发者分发的可重复使用的份额, 在恢复所分享的某一秘密时, 每一分享者先利用自己的份额生成一个子份额, 并把子份额提供给其他合作者. 即使一个分享者的所有子份额都公开, 他的秘密份额也不会被泄露. Harn 的方案在实用中有以下缺点: (1) 每一分享者验证自己的份额的正确性时, 需检验 $n!/((n-t)!\,t!)$ 个等式(其中 n 是分享者的个数, t 是门限值), 而每一个等式都是基于模指数运算的, 计算量很大; (2) 对子份额的有效性的验证是交互式的. 在恢复秘密时, 合作的分享者必须通过交互式的协议来验证他们提交的子份额的有效性. (3) 只有事先确定的秘密才可被分享, 因而在现实中并不实用. Chen[28] 提出的 (t, n) VMSS 方案克服了文[27] 中方案的缺点, 在其中分发者要记录所有分享者的份额, 并对每一秘密计算一个 n 维的检验向量, 这一检验向量用来防止分享者在恢复秘密时欺骗. 为计算此检验向量, 分发者需多花费 $2n$ 次的模指数运算, 计算代价也很大. 文献[29] 提出的 (t, n) VMSS 方案克服了文[27] 和[28] 中的方案的缺点, 并具有下述性质: (1) 可有效地抵抗分发者欺骗. 每一分享者检验自己的份额的正确性只需 t 次模指数运算. (2) 可抵抗分享者欺骗. 在恢复秘密时, 分享者提供的子份额的有效性是可验证的, 且验证过程是非交互式的. (3) 分发者可随意地在分享者中分享任何一组秘密, 而且不需要为恢复秘密增加额外的公开信息. 因此, 就总体而言, 文[29] 中的方案是目前较好的 VMSS 方案, 但其效率仍然不够理想. 文献[65] 提出了一个具有一般接入结构的高效 VMSS 方案, 具有一定的实用价值.

2.5　基于一般接入结构的 VSS 分享方案

已经提出的 VSS 方案主要是门限方案, 只有为数不多的几个非门限方案. 正如文献[14] 所指出的那样, 把 VSS 的概念推广到一般接入结构上去是必要的, 而且有着重要的理论和实用价值. 首先它可以为一般接入结构上的秘密分享提供强健性(robustness, 也称为鲁棒性); 其次, 门限方案只有在所有分享者具有完全平等的地位及可靠性和安全性的情况下才是有意义的, 这种情况在现实中并不多见, 因此对基于一般接入结构的可验证秘密分享的研究具有广泛的现实意义. Benaloh 曾经指出[30], Feldmarr VSS 方案可以推广到一般接入结构上, Stadler 在文[20] 中也提到他给出的基于离散对数的 PVSS 方案可以推广到一般接入结构上, 但他们都未给出具体的细节, 而且这两个方案到一般接入结构上的推广只能达到计算上的安全性而且后者的效率很不理想. Gennaro 在文[14] 中给出了第一个具有非常好的安全性质的具有一般接入结构的 VSS 方案. 但这一方案的结构较为复杂, 分享者需要存储的秘密数据的个数不少于他所属于的最小合格子集的个数, 通信和计算代价都很大, 因此其效率离实用还有一定的差距. 张福泰[65] 对一般接入结构上的 VSS 做了进一步的研究, 提出了几个适用于向量空间接入结构及任意接入结构的高效 VSS 协议.

2.6　泛可验证的秘密分享方案

Mao 中提出以双方协议来实现秘密分享过程的可验证性[31]. 其验证协议在分发者和验证者间进行, 而分享者是脱线的. 验证时, 分发者把各秘密份额用相应的各分享者的公钥加密后发给验证者, 验证者按照一定的方式来验证分享过程的正确性. 这样的验证协议可重复多次, 每次参加执行的验证者可以是不同的, 因而等于无形中给验证者附加了诚实性的要求.

3　在门限密码学中的应用

可验证秘密分享在门限密码学[32] 中得到了广泛的应用[33-61]. 几乎所有实用的门限密码体制都用到了可验证秘密分享.

3.1　分布式的密钥生成方案

分布式的密钥生成[18, 33](Distributed Key Generation, 简称 DKG), 是门限密码系统及分布式密码计算的重要组成部分, 在面向群体的密码学中起着非常重要的作用. 它允许多个参与者共同合作以生成一个密码系统的公钥和私钥, 使得公钥以公开形式输出, 而私钥被参与者按照某一秘密分享方案所分享. 这一被分享的私钥以后可以用于面向群体的密码系统, 如群体签字或群体解密. 对基于离散对数的密码系统, 分布式的密钥生成相当于分享一个随机的来自均匀分布的秘密值 x, 而使 $y = g^x \pmod p$ 公开(p, q 是大素数, $q \mid (p-1)$, g 是 $GF(p)$ 中的一个 q 阶元.). 安全的 DKG 协议还是其它许多分布式协议的重要组成部分, 如基于离散对数的签字协议中随机数的生成协议及 *proactive* 秘密分享中秘密份额的更新协议等.

第一个 DKG 方案是由 Pedersen[33] 于 1991 年提出的. 之后, 该方案被多次修改并被多次用于门限密码学及其应用的研究中[17, 34-40]. Pedersen 的 DKG 协议的基本思想是并行执行 n 次 Feldman 的可验证秘密分享协议, 在其中, 每一参与者 P_i 作为分发者把他随机选择的秘密值 z_i 可验证的在所有参与者中分享, 最终的秘密钥 x 是被正确分享的各 z_i 之和, 最终的公钥 y 是被正确分享的各 z_i 所对应的公开值 $y_i = g^{z_i} \pmod p$ 之积.

文献[18] 对基于离散对数的分布式密钥生成进行了深入研究. 该文献首先给出了安全的 DKG 协议的基本要求, 紧接着指出了文[33] 中的 DKG 协议的安全缺陷, 并给出了一种攻击方法. 恶意的攻击者利用这种方法可操纵秘密钥 x 的输出分布使其与均匀分布大相径庭. 之后, 作者又提出了一个可证明安全的 DKG 协议. 在这一协议中, 不仅使用了 Feldmarr VSS,

而且应用了 Pedersen VSS. 与文[33]中的 DKG 协议相比, 不仅提高了安全性, 而且保持了原协议的高效性. 因而是到目前为止最有实用价值的基于离散对数的分布式密钥生成协议. 对如何分布式的产生 RSA 体制的密钥对, 目前已经提出了几个方案[54,55], 但这些方案的效率都不够理想. 张福泰[66]讨论了基于一般接入结构的分布式密钥生成, 并提出了一个安全高效的 DKG 协议, 可应用于基于一般接入结构的分布式密码系统中.

3.2 在门限签字中的应用

门限签字是门限密码学的重要组成部分. 研究门限签字方案有两方面的目的, 一是增加签字机构的可得到性, 即通过分散签字的权利, 使一个群体的多个子集具有产生合法签字的权利; 二是增加攻击者获取签字私钥从而伪造签字的困难性. 门限签字要求在不对参与签字的任何一方暴露签字私钥的情况下可生成任意多个签字, 而且这些签字与完整地拥有签字私钥的单个签字人所做的签字没有任何区别. 对目前已有的实用的签字方案的门限实现方法的研究是门限签字研究中的主要内容. 文献[41~46]对门限 RSA 签字进行了大量研究, 取得了不少好的结果. 也有许多文献[33~39]涉及了 ElGamal 型的签字方案的门限实现. 文[34]对各种 ElGamal 型的签字方案的门限实现方法进行了小结. 尤其需要提到的是文献[17, 47], 这两篇文章对 DSS 签字的门限实现进行了深入研究, 提出了几个适用于不同安全要求的门限 DSS 签字方案. 在这些方案中, 无论是密钥的分布式生成, 还是部分签字的生成, 最终签字的产生都频繁地使用了可验证秘密分享技术. Feldmarr VSS 方案及 Pedersen VSS 方案在这些门限签字方案的安全性及可行性方面都发挥了极其重要的作用. 由于在这些门限 DSS 方案中, 密钥的分布式生成均采用了文[33]中的方法, 因而也存在着缺陷. 王贵林[66]、王宏[67]、Stinson[68]及 Damgård[69]进一步探讨了一些数字签字的门限生成, 文[65]对签密的门限生成做了较为深入的研究, 提出了一个安全高效的门限签密协议. 以上提到的这些门限签字和门限签密协议在对一些重要而敏感的信息的认证及群体保密认证通信中有着实际应用价值.

4 在多方安全计算中的应用

多方安全计算(Secure Multi-Party Computation, 简称 MPC)的概念是在文献[16]和[48]中提出的, 它要实现的目标是: 使 n 个参与者计算他们各自的秘密输入的一个函数, 要求在即使有恶意攻击者的情况下也要保证输出的正确性和各自的输入的秘密性. 可验证秘密分享是实现多方安全计算的基本工具. 几乎所有的多方安全计算协议都以某种形式的可验证秘密分享为基础[9~16]. 只有文[49]是例外. 文献[50~52]均利用可验证秘密分享技术探讨了安全高效的多方安全计算协议的设计问题. Gennaro 等人在文[19]中给出的基于可验证秘密分享的最基本的多方安全计算协议, 大大提高了乘法的计算速度, 已经受到研究界的普遍重视[12]. 文献[17, 47]基于 Feldmarr VSS 和 Pedersen VSS 方案提出了有限域上求逆的多方安全计算协议. 仍然是基于 VSS, 文献[53]对模数 N 被参与者所分享的情况, 给出了 Z_N^* 中求逆的多方安全计算协议. 这一协议改进了文[54]和[55]中的方法, 在 RSA 密钥的安全分享及基于整数分解的数字签字的分布式生成中起着重要作用. 最近 Hirt 等人[70]着重对多方安全计算中的强健性进行了讨论, 提出了无需增加额外的计算和通信代价就可获得强健性的方法; Cramer 等人[71]对分布式线性代数做了深入研究, 给出了对线性代数中许多问题的分布式解决方法. 这些结果在多方安全计算的理论和应用两方面都有重要的意义.

5 在电子商务中的应用

VSS 在电子商务中的电子现金、电子拍卖、公平交换等方面有着重要应用. Stadler 指出可公开验证秘密分享技术能够应用于可撤消匿名性的电子现金系统的设计中[20]. PVSS 可用来以可信机构的公钥可验证地加密用户跟踪信息. 在这样的电子支付系统中, 通常情况下, 用户是不可跟踪的, 但如果用户利用系统的匿名性进行非法交易或犯罪活动, 那么系统借助于可信机构的帮助, 就可找到用户的真实身份.

电子拍卖是电子商务中极为活跃的一个方面. 已经提出的电子拍卖方案有很多, 其中为数不少的方案采用了 VSS 技术, 如文献[56, 57]中的方案. Harkavy 等人在[56]中给出了一组密封式拍卖协议. 在这些协议中假定了分布式的拍卖代理, 投标及确定中标价的过程中利用了基于 VSS 的安全计算方案. 这些拍卖协议具有几个方面的优点: 投标人的标书即使在拍卖结束后仍然是保密的; 既适用于第一价位拍卖又适用于第二价位拍卖; 效率较高, 具有实用价值. 文献[57]中也是利用基于 VSS 的安全计算提出了适用于第二价位拍卖的网上电子拍卖方案. 这一方案能够对除了中标人之外的所有投标人的标书保密, 并具有较高的效率.

公平交换是电子商务中的一个非常重要的问题. 一般情况下, 公平交换协议中都涉及了可信的第三方. 对可信第三方的信赖程度分为完全可信和半可信两种类型. 在基于完全可信的第三方的公平交换协议中, 可信第三方是系统的瓶颈, 而且交易双方的秘密会完全泄露给可信第三方. 具有半可信第三方的公平交换协议, 需要较小的通信量, 且能够保护交易双方的隐私, 因而更为实用. Franklin 等人在文[58]中, 应用 VSS 技术, 设计了一种基于半可信第三方的公平交换协议. 其特点在于, 除非交易双方主动把秘密告诉第三方, 否则, 第三方不可能知道交易的具体内容. 蒋晓宁等人在文[59]中, 基于 PVSS 的理论, 提出了一个具有半可信第三方的公平交换协议, 除了具有较高的效率外, 还具有半可信第三方只需离线工作及交易双方的秘密始终对第三方保密等好的性质. 张福泰[65]基于 PVSS 提出了具有分布式半可信第三方的最优公平交换协议, 分布式的半可信第三方使得协议的公平性和公正性具有独到的优点.

除了以上所谈到的应用外, VSS 在密钥托管[60,21]、可验证签字分享[61]及电子选举[22]等方面也有着重要的应用.

6 发展趋势及几个值得重视的研究方向

由上面的阐述和分析可以看出, 可验证秘密分享(VSS)在

密码学和信息安全中发挥着重要的、不可替代的作用. 目前, 可验证秘密分享的研究无论是在理论上, 还是在应用方面都取得了较丰富的成果. 同时, 该领域的研究也正在蓬勃发展. 从最近一年多该领域所取得的成果来看, 发展趋势将是: 对安全高效的各种可验证秘密分享协议(包括广义 *VSS* 协议)的研究, 以及对 *VSS* 在面向群体的密码学、安全计算及电子商务等诸多领域的广泛应用的研究. 下面列出我们认为值得重视的几个研究方向, 供对该领域有兴趣的研究人员参考:

(1)信息论安全(无条件安全)的可验证秘密分享算法的研究. 信息论安全(无条件安全)的可验证秘密分享算法在理论和应用两方面都有着重要价值, 但到目前为止, 这样的算法仅有为数不多的几个.

(2)安全、高效的可公开验证的秘密分享(PVSS)方案的设计. 已有的涉及可公开验证的秘密分享及其应用的文献只有文[20~22]等很少的几篇, 这对 PVSS 的广泛应用是一个限制.

(3)具有一般接入结构的可验证秘密分享(广义 VSS)方案的研究. 门限可验证秘密分享方案在无形中附加了参与秘密分享的各方具有平等的地位和权利的条件, 而在现实中有很多场合, 不能使这样的条件得到满足. 基于一般接入结构的分布式数字签字、分布式安全计算都需要广义 VSS 支持. 因此有必要对具有非门限接入结构的 VSS 方案的设计和分析进行研究, 以满足实际应用的需要. 现有的非门限 *VSS* 方案很少且效率都不够理想.

(4)可验证秘密分享在可撤消匿名性的电子现金系统及最优公平交易中的应用. 虽然 Stadler 在文[20]中已经指出, PVSS 能用于可撤消匿名性的电子现金系统中, 但到目前为止还未看到基于 PVSS 的可撤消匿名性的电子现金方案. PVSS 在公平交易中的应用也只有文[58, 59, 65]等很少的几篇文献有所涉及.

(5)签密及 Esign 等签字方案的基于 VSS 的门限实现. 对 RSA 及 ElGamal 型的签字方案的门限实现在文献中较为多见, 对签密的门限生成仅有文献[65]有所涉及, 而对 Esign 等重要签字方案的门限实现在现有文献中还见不到, 这对这些签字方案在群体通信等场合的应用是一个限制.

(6)探索 VSS 在其它方面的新的应用.

7　结束语

可验证秘密分享(VSS)在信息安全和数据保密中起着非常重要的作用, 是设计多方安全协议的基本工具. 自从其概念于 1985 年被提出后, 受到了密码学和信息安全界的普遍关注, 到现在为止已经取得了大量的研究成果. 一些好的 VSS 方案已经被广泛地应用于诸如多方安全计算、密钥托管、门限密码学、电子商务及电子选举等多个研究领域. 本文全面总结并评述了可验证秘密分享及其应用方面所取得的研究成果, 探讨了该领域研究的发展趋势. 在深入分析的基础上, 最后指出了我们认为值得重视的几个研究方向.

参考文献:

[1] Shamir, A. How to share a secret[J]. Communications of the ACM, 1979, 24(11): 612- 613.

[2] Blakley, G R Safeguarding cryptographic keys [A]. Proceedings of the National Computer Conference[C], Montvale: NCC, 1979.

[3] Kamin E D., Green J W., Hellman M E., On secret sharing systems [J]. IEEE Trans., 1983, IT-29(1): 35- 41.

[4] Benloh J C., Secret sharing homomorphisms: Keeping shares of a secret secret [A]. Advances in cryptology-CRYPTO' 86 [C]. California: CRYPTO, 1986.

[5] Carpentieri M., A perfect threshold secret sharing scheme to identify cheaters [J]. Des., Code CRYptogr., 1995, 5(3): 183- 187.

[6] Chor B, Goldwasser S. Verifiable secret sharing and achieving simultaneity in the presence of faults [A]. Proceedings of 26th IEEE symposium on Foundations of computer science [C]. Portland: IEEE, 1985.

[7] Feldman P A practical scheme for norr interactive verifiable secret sharing [A]. Proceedings of 28th IEEE symposium on Foundations of Comrputer Science [C]. Canada: IEEE, 1987.

[8] Pedersen T P. Norr interactive and informatiorr theoretic secure verifiable secret sharing [A]. CRYPTO' 91 [C]. California: CRYPTO, 1991.

[9] Berr or M, Goldwasser S, Widgerson A. Completeness theorems for norr cryptographic fault-tolerant distributed computation [A]. Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing[C]. Chicago: ACM, 1988.

[10] Chaum D, Crépeau C, Damgård I. Multiparty unconditionally secure protocols [A]. Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing [C]. Chicago: ACM, 1988.

[11] Cramer R, Van Damgaard I, Maurer U. General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme [A]. EUROCRYPT' 2000 [C]. Beligum: CRYPT, 2000.

[12] Cramer R. Introduction to secure computation [A]. Lectures on Data Security, Modern Cryptology in Theory and Practice [C]. Springer, Berlin, 1999.

[13] Gennaro R., Micali S. verifiable secret sharing as secure computation [A]. EUROCRYPT' 95 [C]. Fance: EUROCRYPT, 1995.

[14] Gennaro R. Theory and practice of verifiable secret sharing [D]. Ph. D. Thesis, MIT, 1996.

[15] Rabin T, Berr or M. Verifiable secret sharing and multi party protocols with honest majority [A]. Proc. ACM STOC' 89 [C]. Seattle: ACM, 1989.

[16] Goldreich O, Micali S, Wigderson A. How to play an mental game or a completeness theorem for protococls with honest majority [A]. Proc. Of ACM STOC' 87 [C]. New York: ACM, 1987. 218- 229.

[17] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Robust threshold DSS signatures [A]. EUROCRYPT' 96 [C]. Springer-Verlag, Berlin: EUROCRYPT, 1996.

[18] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Secure distributed key generation for discrete-log based cryptosystems [A]. EUROCRYPT' 99 [C]. Springer-Verlag: EUROCRYPT, 1999.

[19] Gennaro R, Rabin M, Rabin T. Simplified VSS and fast-track multiparty

computations with applications to threshold cryptography [A]. Proceedings of the 1998 ACM Symposium on Principles of Distributed Computing [C]. Puerto Vallarta, Mexico: ACM, 1998.

[20] Stadler M, Publicly verifiable secret sharing, In Advances in cryptology [A]. EUROCRYPT' 96 [C]. Springer-Verlag, Berlin: EUROCRYPT, 1996.

[21] Fujisaki E, Okamoto T. A practical and provably secure scheme for publicly verifiable secret sharing and its applications [A]. Advances in Cryptology, EUCRYPTO' 98 [C]. Finland: EURCUYPTO, 1998.

[22] Schoenmakers B. A simple publicly verifiably secret sharing scheme and its application to electronic voting [A]. CRYPTO' 99 [C]. Springer-Verlag, Berlin: crypto, 1999.

[23] Zheng Y, Hardjono T, Seberry J. Reusing shares in secret sharing schemes [J]. Comput. J., 1994, 37(3): 199– 205.

[24] He J, Dawson E. Multistage secret sharing based on one-way function [J]. Electron. Lett., 1994, 30(19): 1591– 1592.

[25] He J, Dawson E. Multisecret-sharing scheme based on one-way function [J]. Electron. Lett., 1995, 31(2): 93– 95.

[26] Jackson W. A, Martin K. M, O' keefe M. Multisecret threshold schemes [A]. CRYPT' 93 [C]. Springer-Verlag, Berlin: CRYPT, 1993.

[27] Harn L. Efficient sharing (broadcasting) of multiple secrets [J]. IEE Proc. Comput. Digit. Tech., 1995, 142(3): 237– 240.

[28] Chen L, Gollmann D, Mitchell C J, Wild P. Secret sharing with reusable polynomials [A]. Proc. Of the second Australisian Conference on Information Security and Privacy– – – ACISP' 97 [C]. Australia: ACISP, 1997.

[29] Lin T Y, Wu T C. (t, n) threshold verifiable multisecret sharing scheme based on factorization intractability and discrete logarithm modulo a composite problems [J]. IEE Proc. – Comput. & Digit. Tech. 1999, 146(5): 264– 268.

[30] Benaloh J, Leichter J. Generalized secret sharing and monotone functions [A]. Proc. CRYPTO' 88 [C]. Barbara: CRYPTO, 1988.

[31] Mao W. Necessity and realization of universally verifiable secret sharing [A]. IEEE Symposium on Security and Pricacy [C]. Oakland, USA: IEEE, 1998.

[32] Desmedit Y, Frankel Y. Threshold Cryptosystem [A]. CRYPTO' 89 [C]. Barbara: crypto, 1989.

[33] Pedersen T. A threshold cryptosystem without a trusted party [A]. EUROCRYPT' 91 [C]. UK: ROCRYPT, 1991.

[34] Cerecedo M, Matsumoto, Imai H. Efficient and secure multiparty generation of digital signatures based on discrete logarithms [J]. IEICE Trans. Fundamentals, 1993, E76– A(4): 532– 545.

[35] Harn L. Group oriented (t, n) digital signature scheme [J]. IEE Proc. Comput. Digit. Tech, 1994, 141(5): 307– 313.

[36] Li G-H, Hwang T, Lee N-Y. (t, n) threshold signature schemes based on discrete logarithm [A]. EUROCRYPT' 94 [C]. Italy: EUROCRYPT, 1994.

[37] Herzberg A, Jakobsson M, *et al*. Proactive public key and signature systems [A]. 4th ACM Conference on Computers and Communication Security [C]. Zurich, Switzerland: ACM Press, 1997. 100– 110.

[38] Park C, Kurosawa. New ElGamal type threshold digital signature scheme [J]. IEICE Trans Fundamentals, 1996, E79-A(1): 86– 93.

[39] Shoup V, Gennaro R. Securing threshold cryptosystems against chosen ciphertext attack [A]. EUROCRYPT' 98 [C]. Finland: EUROCRYPT, 1998.

[40] Cramer R, Gennaro R, Schoenmakers [A]. A secure and optimally efficient multi-authority election scheme. EUROCRYPT' 97 [C]. German: EUROCRYPT, 1997.

[41] Desmedt Y, Frankel Y. Shared generation of authenticators and signatures [A]. CRYPTO' 91[C]. Barbara: CRYPTO, 1991.

[42] De Santis A, Desmedt Y, Frankel Y, Yung M. How to share a function securely [A]. Proc. 26th ACM Symp. On Theory of Computing [C]. New York: IEEE, 1994.

[43] Frankel Y, Gemmel P, Yung M. Witness-based cryptographic program checking and robust function sharing [A]. Proc. 28th ACM Symp. On Theory of Computing [C]. Philadelphia: ACM, 1996.

[44] Gennaro R, Jarecki S, *et al*. Robustand efficient sharing of RSA functions [A]. CRYPTO' 96 [C]. Barabara: CRYPTO, 1996.

[45] Rabin T. A simplified approach to threshold and proactive RSA [A]. CRYPTO' 98 [C]. Barbara: CRYPTO, 1998.

[46] Shoup V. Practical threshold signaturs [A]. EUROCRYPT' 2000 [C]. Belgium: EUROCRYPT, 2000.

[47] Gennaro R, Jarecki S, *et al*. Robust threshold DSS signatures [J]. Information and Computation, 164, 2001: 54– 84.

[48] Yao A C. Protocols for secure computations [A]. 23rd Annual Symporsium on Foundations of Computer science [C]. Chicago: ASFC, 1987.

[49] Franklin M, Harber S. Joint encryption and message-efficient secure computation [J]. Journal of Cryptology, 1996, 9(4): 217– 232.

[50] Cramer R, Damgård I, Nielsen J B. Multi-party computation from threshold homomorphic encryption [A]. EUROCRYPT' 01 [C]. Australia: EUROCRYPT, 2001.

[51] Cramer R, Damgård I, Dziembowski S, Hirt M, Rabin T. Efficient multiparty computations secure against an adaptive adversary [A]. EUROCRYPT' 99 [C]. Prague: CRYPT, 1999.

[52] Hirt M, Maurer U, Przydatek B. Efficient secure multi-party computation [A]. Asiacrypt' 2000 [C]. Japan: Asicrypt, 2000.

[53] Catalano D, Gennaro R, Halevi S. Computing inverses over a shared secret modulus [A]. EUROCRYPT' 2000 [C]. Bruges: EUROCRYPT, 2000.

[54] Boneh D, Franklin M. Efficient generation of shared RSA keys [A]. CRYPT' 97 [C]. Barbara: CRYPT, 1997.

[55] Frakel Y, Mckenzie P, Yung M. Robust efficient distributed RSA-key generation [A]. STOC' 98 [C]. Dallas: STOC, 1998.

[56] Harkavy M, Kikuch H, Tygar J D. Electronic auctions with private bids [A]. Proc of the 3rd USENIX Workshop on ElectronicCommerce [C]. Massachusetts, USA: USENIX, 1998.

[57] Kikuchi H, Harkavy M, Tygar J D. Multi-round anonymous auction protocols [A]. Proc. Of the first IEEE workshop on dependable and real time E– Commerce Systems [C]. New York: IEEE, 1998.

[58] Franklin M K, Reiter M K. Fair exchange with a semi-trusted third party [A]. Proc. of 4th ACM Conf. on Computer and Communication Security [C]. Zurich, Switzerland, ACM Press: 1997.

[59] 蒋晓宁, 叶澄清, 潘雪增. 基于半可信离线第三方的公平交易协议 [J]. 计算机研究与发展, 2001, 38(4): 502– 508.

[60] Denning D E, Smid M. Key escrowing today [J]. IEEE Communications, 1994, 32(9): 58– 68.

[61] Franklin M K, Reiter M K. Verifiable signature sharing [A]. EUROCRYPT' 95 [C]. Fance: EUROCRYPT, 1995.

[62] Mu Yi, Varadharajan V. A fail-stop verifiable secret sharing scheme [A]. International Workshop on Cryptology and Network Security [C]. Taipei, Taiwan: IWCNS, 2001.

[63] Pieprzyk J, Zhang Xiarr Mo. Nonlinear secret sharing immune against cheating [A]. International Workshop on Cryptology and Network Security [C]. Taipei, Taiwan: IWCNS, 2001.

[64] Zhang Xiarr Mo. Cheating immune secret sharing [A]. 3nd International Conference on Information and Communications Security, ICICS' 01, LNCS, 2229 [C]. China: ICICS, 2001.

[65] 张福泰. 可验证秘密分享及其应用研究 [D]. 西安: 西安电子科技大学, 2001.

[66] 王贵林. 门限签名方案和认证协议的设计与分析 [D]. 北京: 中国科学院软件研究所, 2000.

[67] 王宏. 可验证秘密共享及门限密码体制研究 [D]. 西安: 西安电子科技大学, 2001.

[68] Stinson D R, Strobl R. Provably secure distributed schnorr signatures and a (t, n) threshold scheme for implicit certificates [A]. ACISP 2001 [C]. Australia: ACISP, 2001.

[69] Damgård I, Koprowski M. Practical threshold RSA signatures without a trusted dealer [A]. LNCS, 2045 [C]. Springer-Verlag, Berlin: LNSC, 2001.

[70] Hirt M, Maurer U. Robustness for free in unconditional multi-party computation [A]. LNCS, 2139 [C]. Springer-Verlag, Berlin: LNCS. 2001.

[71] Cramer R, Damgård I. Secure distributed linear algebra in a constant number of rounds [A]. LNCS, 2139 [C]. Springer-Verlag, Berlin: LNCS, 2001.

[72] Ayako Maeda, Atsuko Miyaji, and Mitsuru Tada. Efficient and unconditionally secure verifiable threshold changeable scheme [A]. ACISP 2001 [C]. Australia: ACISP, 2001.

作者简介:

张福泰　男, 1965 年 8 月出生于陕西省陇县, 2001 年获密码学专业博士学位, 现为南京师范大学数学与计算机科学学院副教授, 主要研究兴趣为信息安全及电子商务. Email: Zhangfutai@263.net, ffttzhang@hotmail.com

赵福祥　男, 1966 年 4 月出生于陕西省西安市, 1992 年获计算机科学专业硕士学位现为西安电子科技大学密码学专业博士研究生, 主要研究兴趣为信息安全及电子商务.

王育民　男, 1938 年 2 月出生于北京市, 现为西安电子科技大学教授, 博士生导师, IEEE 高级会员, 长期从事信息论和通信安全方面的教学和研究工作, 取得了大量研究成果.