Journal of Computer Applications
计算机应用,2013,33(5):1391 - 1393
ISSN 1001-9081
CODEN JYIIDU
2013-05-01
http://www.joca.cn

文章编号:1001 - 9081(2013)05 - 1391 - 03
doi:10.3724/SP.J.1087.2013.01391

基于线性单向函数的可验证的多秘密共享方案

张晓敏*
(陕西省行政学院 基础理论教研部,西安 710068)
(*通信作者电子邮箱 zhangxiaomin81@163.com)

摘　要:基于 Shamir 的门限秘密共享方案和线性单向函数的安全性以及离散对数问题的困难性,提出了一个可验证的多秘密共享方案。该方案中每个参与者只需保护一个秘密份额,就可共享多个秘密。秘密恢复之前,参与者可验证其他参与者所提供的影子份额的正确性。秘密恢复后,参与者的秘密份额不会泄露,可重复使用,并且所需的公开参数较少,秘密分发过程不需要安全信道。

关键词:秘密共享;可验证秘密共享;多秘密共享;双线性映射;线性单向函数
中图分类号:TP309.7　　**文献标志码**:A

Verifiable multi-secret sharing scheme based on linear one-way function

ZHANG Xiaomin*
(*Department of Basic Courses, Shaanxi Administration School, Xi'an Shaanxi* 710068, *China*)

Abstract: Based on Shamir's threshold secret sharing scheme, the security of the linear one-way function and the difficulty of the discrete logarithm problem, a verifiable multi-secret sharing scheme was proposed. In this scheme, each participant needed just one secret share to share a set of secrets. Before recovering the secrets, participants could verify the correctness of the shadow shares provided by other participants. After recovering all of the secrets, the secret shares of the participants were still kept confidential and the secret shares could be used to share a new set of secrets. At the same time, the proposed scheme had fewer public parameters, and it did not require secure communication channels.

Key words: secret sharing; veriable secret sharing; multi-secret sharing; bilinear map; linear one-way function

0　引言

现代密码体制的安全性取决于密钥的安全性,秘密共享方案是密钥管理的有效途径,也是信息安全和数据保密的重要手段。1994 年,He 等[1]首先将 Shamir 的秘密共享思想[2]和公开移动技术结合,提出了多秘密共享方案,每个参与者只持有一个秘密份额,却可以共享多个秘密。但该方案要求参与者必须按预先指定的顺序恢复秘密,这在实际应用中是难以令人满意的;此外,在 n 个参与者中共享 m 个秘密,该方案需要公开参数 $m \times n$ 个,增加了系统的存储难度,一定程度上影响了方案的有效性。Harn[3] 将文献[1]中的方案进行了改进,将公开参数的个数减少至 $m \times (n-t)$。1995 年,He 等[4]又利用单向函数提出了一个新的多秘密共享方案,参与者可不按预先指定顺序恢复秘密,但是公开参数增加至 $m \times (n+1)$ 个。2005 年,在 Chang 等[5]提出的多秘密共享方案中,即使所有秘密恢复以后,参与者的秘密份额仍然是保密的,也就是说,参与者可用此秘密份额共享另一组秘密。该方案拓展了秘密共享的应用范围,有重要的应用价值,但是此方案中参与者仍需要按特定顺序恢复秘密,且公开参数依然是 $m \times n$ 个。这些秘密共享方案存在的共同问题是不能很好地抵抗参与者的欺诈,即不诚实的参与者在恢复秘密时会提供虚假的秘密份额,从而使一些合法参与者不能恢复出正确的秘密。Chor 等[6]提出的可验证秘密共享的概念可解决这一问题。可验证秘密共享方案是在通常的秘密共享方案上附加了一个验证算法而构成的。目前,研究者已经提出了各种可验证的秘密共享方案[7-10]。文献[11]中,Harn 提出了一种 (t,n) 门限可验证秘密共享方案,该方案中参与者验证秘密份额时计算量过大;Lin 等[12]基于离散对数问题提出了一种改进的方案,但 He 等[13]指出该方案存在参与者欺骗,Chang 等[14]提出的方案避免了这种欺骗,但是事实上,该方案也存在安全漏洞,且密钥分配阶段需要安全信道,增加了系统的传输困难。本文在此基础上,利用双线性映射[15]和线性单向函数[16],基于 Shamir 门限秘密共享方案和离散对数问题的困难性,提出一个新的可验证多秘密共享方案,该方案在秘密分配阶段不需要安全信道,参与者在秘密恢复前可验证其他参与者提供的影子份额的正确性。

1　预备知识

下面首先介绍双线性映射和线性单向函数的概念。

定义 1[12]　双线性映射。设 q 是一个大素数,G 是阶为 q 的加群,G_1 是阶为 q 的乘群,映射 $e: G \times G \to G_1$ 称为双线性映射,如果满足以下条件:

1) 双线性性:$\forall P,Q,R \in G_1$, $\forall a,b \in \mathbf{Z}_q^*$,有 $e(aP,bQ) = e(P,Q)^{ab}$,$e(P+R,Q) = e(P,Q)e(R,Q)$;

2) 非退化性:若 $\forall Q \in G_1$,$e(P,Q) = 1$,则 $P = 0$;

3) 可计算性:$\forall P,Q \in G_1$,存在有效算法可以计算 $e(P,Q)$。

定义 2[13]　线性单向函数。设 G 是一个阶为 q 的加群,其中 q 是安全的大素数,映射 $h: G \times \mathbf{Z}_q^* \to G$ 称为线性单向函数,如果满足以下条件:

1) 对于任意的 $P \in G$ 和 $x \in \mathbf{Z}_q^*$,给定 $h(P,x)$ 和 x,无法在多项式时间内得到 P;

2) 对于任意的 $P \in G$ 和 $a,x \in \mathbf{Z}_q^*$,有 $h(aP,x) = ah(P,x)$;

收稿日期:2012-11-20;**修回日期**:2012-12-26。
作者简介:张晓敏(1981 -),女,甘肃白银人,助教,硕士,主要研究方向:密码学、信息安全。

3) 给定 $P \in G, x, \{x_i \in \mathbf{Z}_q^* \mid i = 1,2,\cdots,n\}$ 及 $\{(x_i, h(aP, x_i)) \mid i = 1,2,\cdots,n\}$，无法在多项式时间内得到 $h(aP, x)$。

定义 3[12] 离散对数问题。设 G 是一个加群，P 是 G 的生成元，给定 $Q \in G$，寻找 $x \in \mathbf{Z}_q^*$ 使 $Q = aP$ 成立。

文献[12]指出，如果存在双线性映射 $e: G \times G \to G_1$，则，群 G 上的离散对数问题是困难问题。

2 可验证的多秘密共享方案

下面本文利用双线性映射和线性单向函数，基于 Shamir 门限秘密共享方案，提出一个可验证的多秘密共享方案，该方案是一个 (t,n) 门限方案。

2.1 系统初始化

假设 q 是安全的大素数，G 是一个阶为 q 的加群，其元素是椭圆曲线上的点，P 是 G 的生成元，映射 $e: G \times G \to \mathbf{Z}_q^*$ 是双线性映射，映射 $h: G \times \mathbf{Z}_q^* \to G$ 是线性单向函数，$P_1, P_2, \cdots, P_n$ 是 n 个参与者，$S_1, S_2, \cdots, S_m \in G$ 是要共享的 m 个秘密，$x_1, x_2, \cdots, x_n \in \mathbf{Z}_q^*$ 是参与者的固定参数。

2.2 秘密发布阶段

假设要在 n 个参与者 $P_1, P_2, \cdots, P_n$ 中共享 m 个秘密 $S_1, S_2, \cdots, S_m$，执行以下步骤：

1) 分发者随机选取 $r \in \mathbf{Z}_q^*$，计算并公开 $Q = rP$；

2) 每个参与者 P_j 随机选择计算 $s_j \in \mathbf{Z}_q^*$ 作为其秘密份额，并通过公开信道向分发者发送 $s_jQ, j = 1,2,\cdots,n$；

3) 分发者收到所有 s_jQ 后，首先确保每个参与者发送的 s_jQ 是不同的，然后通过等式 $r^{-1}(s_jQ) = r^{-1}(s_jQrP) = s_j(r^{-1}r)P = s_jP$ 计算出 $s_jP (j = 1,2,\cdots,n)$；

4) 分发者计算 $Q(0)P = \sum_{j=1}^{n}\left(\prod_{i=1,i\neq j}^{n}\frac{x_i}{x_i - x_j}\right)s_jP$，其中 $Q(x)$ 是通过点 $(x_1,s_1), (x_2,s_2), \cdots, (x_n,s_n)$ 的 $n-1$ 次 Lagrange 插值多项式；

5) 分发者计算并公开 $Q(d_k)P = \sum_{j=1}^{n}\left(\prod_{i=1,i\neq j}^{n}\frac{d_k - x_i}{x_j - x_i}\right)s_jP$，$k = 1,2,\cdots,n-t$，其中 d_k 是集合 $\{1,2,\cdots,q-1\}/\{x_j \mid j = 1,2,\cdots,n\}$ 中 $n-t$ 个最小的值；

6) 分发者计算 $\alpha_j = h(Q(0)P, j)$ 及 $\beta_j = S_j - \alpha_j$，并公开 $\beta_j (j = 1,2,\cdots,m)$。

2.3 秘密重构阶段

假设 t 个参与者 $P_1, P_2, \cdots, P_t$ 想合作重构秘密 $S_i, i \in \{1,2,\cdots,m\}$，可执行以下步骤：

1) 每个参与者 P_j 首先利用其秘密份额 s_j 计算 $h(s_jP, i)$ 作为其影子份额，$j = 1,2,\cdots,t$；

2) 参与者 $P_1, P_2, \cdots, P_t$ 根据每个参与者提供的影子份额 $\{h(s_jP,i) \mid j = 1,2,\cdots,t\}$ 首先计算

$$\gamma_i = \sum_{j=1}^{t}\left(\prod_{i=1,i\neq j}^{t}\frac{x_i}{x_i - x_j}\right)\left(\prod_{i=1}^{n-t}\frac{d_i}{d_i - x_j}\right)h(s_jP,i) + \sum_{j=1}^{n-t}\left(\prod_{i=1,i\neq j}^{n-t}\frac{d_i}{d_i - d_j}\right)\left(\prod_{i=1}^{t}\frac{x_i}{x_i - d_j}\right)h(Q(d_j)P,i)$$

然后利用公开参数 β_i，计算 $\beta_i + \gamma_i$，即可得到秘密 $S_i, i \in \{1,2,\cdots,m\}$。

2.4 秘密验证阶段

t 个参与者 $P_1, P_2, \cdots, P_t$ 在联合计算 γ_i，恢复秘密 S_i 之前，每个参与者首先验证等式 $e(h(s_jP,i), Q) = e(h(P,i), s_jQ)$ 是否成立，其中 $j = 1,2,\cdots,t$，如果等式成立，则参与者确信其余参与者所提交的影子份额是正确的。

3 方案分析

本文提出的多秘密共享方案的安全性基于 Shamir 门限秘密共享方案、双线性映射与线性单向函数的性质，分析如下：

定理 1 秘密重构阶段 t 个参与者 $P_1, P_2, \cdots, P_t$ 计算得到的秘密是正确的。

证明 秘密发布阶段公开的信息为 $\beta_i = S_i - \alpha_i$，即 $S_i = \beta_i + \alpha_i$，而秘密重构阶段 t 个参与者 $P_1, P_2, \cdots, P_t$ 联合计算

$$\gamma_i = \sum_{j=1}^{t}\left(\prod_{i=1,i\neq j}^{t}\frac{x_i}{x_i - x_j}\right)\left(\prod_{i=1}^{n-t}\frac{d_i}{d_i - x_j}\right)h(s_jP,i) + \sum_{j=1}^{n-t}\left(\prod_{i=1,i\neq j}^{n-t}\frac{d_i}{d_i - d_j}\right)\left(\prod_{i=1}^{t}\frac{x_i}{x_i - d_j}\right)h(Q(d_j)P,i) =$$

$$h\left(\left(\sum_{j=1}^{t}s_j\left(\prod_{i=1,i\neq j}^{t}\frac{x_i}{x_i - x_j}\right)\left(\prod_{i=1}^{n-t}\frac{d_i}{d_i - x_j}\right) + \sum_{j=1}^{n-t}Q(d_j)\left(\prod_{i=1,i\neq j}^{n-t}\frac{d_i}{d_i - d_j}\right)\left(\prod_{i=1}^{t}\frac{x_i}{x_i - d_j}\right)\right)P,i\right) = h(Q(0)P,i) = \alpha_i$$

因此，$\beta_i + \gamma_i = \beta_i + \alpha_i = S_i$，$t$ 个参与者 $P_1, P_2, \cdots, P_t$ 联合计算得到的秘密是正确的。

定理 2 任何人无法在多项式时间内从已恢复的秘密中得到关于未恢复秘密的任何信息。

证明 假设秘密 $\{S_i\}_{i\in I}, I \subset \{1,2,\cdots,m\}$ 已经恢复，那么对于不诚实的参与者而言，$\{\alpha_i = h(Q(0)P,i)\}_{i\in I}$ 是已知的，但由于 $h: G \times \mathbf{Z}_q^* \to G$ 是线性单向函数，由线性单向函数的性质 1，攻击者无法在多项式时间内由 $\{\alpha_i = h(Q(0)P, i)\}_{i\in I}$ 直接得到 $Q(0)P$，因此也无法利用 $Q(0)P$ 计算 $\alpha_k = h(Q(0)P,k) (k \notin I)$；另一方面根据线性单向函数的性质 3)，攻击者无法在多项式时间内由 $\{\alpha_i = h(Q(0)P,i)\}_{i\in I}$ 计算 $\alpha_k = h(Q(0)P,k) (k \notin I)$，因而不诚实的参与者无法通过计算 $\beta_k + \alpha_k$ 得到关于未恢复秘密 S_k 的任何信息。因此，任何人无法在多项式时间内从已恢复的秘密中得到关于未恢复秘密的任何信息。

定理 3 任何人无法在多项式时间内从已恢复的秘密中得到任何关于参与者的秘密份额的信息，秘密验证阶段也不会泄露任何关于参与者的秘密份额的信息。

证明 首先，无论在秘密重构阶段还是秘密验证阶段，每个参与者都只提交了自己的影子份额，并没有提交自己的秘密份额。其次，假设秘密 $\{S_i\}_{i\in I}, I \subset \{1,2,\cdots,m\}$ 已经恢复，那么 $\{h(s_jP,i)\ 1 \leqslant j \leqslant n\}_{i\in I}$ 是已知的，但由于 $h: G \times \mathbf{Z}_q^* \to G$ 是线性单向函数，由线性单向函数的性质 1)，攻击者无法在多项式时间内由 $\{h(s_jP,i)\ 1 \leqslant j \leqslant n\}_{i\in I}$ 直接得到参与者的秘密份额 s_j。同理，在秘密验证阶段，攻击者也无法由参与者提供的影子份额 $\{h(s_jP,i)\}$ 得到参与者的秘密份额 s_j；另一方面，虽然 $s_jQ (j = 1,2,\cdots,n)$ 是通过安全信道发送的，但由于群 G 上的离散对数问题是困难问题，任何人无法从 s_jQ 得到参与者的秘密份额 s_j。因此，任何人无法在多项式时间内从已恢复的秘密中得到任何关于参与者的秘密份额的信息，秘密验证阶段也不会泄露任何关于参与者的秘密份额的信息。

定理表明，秘密恢复后，参与者的秘密份额仍是保密的，可以用来共享另外一组秘密，避免了重复分发秘密份额所带来的计算，提高了方案的利用率。

定理 4 任何少于 t 个参与者合谋，无法在多项式时间内得到关于秘密 $S_i, i \in \{1,2,\cdots,m\}$ 的任何信息。

证明 假设 $t-1$ 个不诚实的参与者合谋恢复秘密 S_i，

$i \in \{1,2,\cdots,m\}$,根据定理 1,任何人无法在多项式时间内从已恢复的秘密中得到关于未恢复秘密的任何信息,因此,不失一般性,不妨假设 S_i 是第一个要恢复的秘密。为了恢复秘密 S_i,不诚实的参与者需要计算 $Q(0)P$ 或者 $h(Q(0)P,i)$。通过多项式 $Q(x)$ 计算 $Q(0)P$,需要知道至少 t 个影子份额 $\{h(s_jP,i)\}$ 的值,而 $t-1$ 个参与者只知道 $t-1$ 个秘密份额影子份额 $\{h(s_jP,i)\}$,由 Shamir 门限秘密共享方案的基本性质可知,这是不可能的。

本文提出的可验证的多秘密共享方案中,在 n 个参与者中共享 m 个秘密,系统需要公开参数 $Q,P,s_jQ(j=1,2,\cdots,n),x_j(j=1,2,\cdots,n),d_k(k=1,2,\cdots,n-t),Q(d_k)P(k=1,2,\cdots,n-t),\beta_j(j=1,2,\cdots,m)$,共 $2(2n+1)+m-2t$ 个,大大降低了系统的存储成本。

4　结语

可验证秘密共享是安全密码协议的重要组成部分,是解决重要敏感信息的安全存储、合法恢复及利用的有效方法。所以,对可验证多秘密共享及其应用的研究具有不可低估的理论与应用价值。本文基于 Shamir 的 (t,n) 门限秘密共享方案和线性单向函数的安全性及离散对数问题的困难性,提出了一个可验证的多秘密共享方案,参与者在秘密恢复前可验证其他参与者提供的影子份额的正确性,并且秘密重构不会泄露参与者的秘密份额,秘密分配阶段不需要安全信道,扩展了方案的应用环境,在密钥管理协议中有很好的应用前景。

参考文献:

[1] HE J, DAWSON E. Multi-stage secret sharing scheme based on one-way function [J]. Electronic Letters, 1994, 30(19): 1591 – 1594.

[2] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22 (11): 612 – 613.

[3] HARN L. Comment: multistage secret sharing scheme based on one-way function [J]. Electronic Letters, 1995, 31(4): 262 – 262.

[4] HE J, DAWSON E. Multisecret sharing scheme based on one-way function[J]. Electronic Letters, 1995, 31(2): 93 – 95.

[5] CHANG T, HWANG M, YANG W. A new multi-stage secret sharing scheme using one-way function[J]. ACM SIGOPS Operating Systems Review, 2005, 39(1): 48 – 55.

[6] CHOR B, GOLDWASSER S, MICALI S, *et al*. Verifiable secret sharing and achieving simultaneity in the presence of faults [C]// SFCS '85: Proceedings of the 26th Annual Symposium on Foundations of Computer Science. Washington, DC: IEEE Computer Society, 1985: 383 – 395.

[7] 田有亮, 马建峰, 彭长根, 等. 椭圆曲线上的信息论安全的可验证秘密共享方案[J]. 通信学报, 2011, 32(12): 96 – 102.

[8] 张恩, 蔡永泉. 基于双线性对的可验证的理性秘密共享方案[J]. 电子学报, 2012, 40(5): 1050 – 1054.

[9] 张利远, 张恩. 基于中国剩余定理的可验证理性秘密共享方案[J]. 计算机应用, 2012, 32(11): 3143 – 3146.

[10] 张建中, 侯建春. 一个新的可验证的(t, n)多秘密共享方案[J]. 陕西师范大学学报: 自然科学版, 2012, 40(5): 1 – 4.

[11] HARN L. Efficient sharing(broadcasting) of multiple secret[J]. Computer and Digitial Techniques, 2005, 152(3): 237 – 240.

[12] LIN T Y, WU T C. (t, n) threshold verifiable multi-secret sharing scheme based on factorization intractability and discrete logarithm modulo a composite problem [J]. Computer and Digitial Techniques, 2009, 156(5): 264 – 268.

[13] HE W H, WU T S. Comment on Lin-Wu (t, n)-threshold verifiable multi-secret sharing scheme[J]. Computer and Digitial Techniques, 2011, 158(3): 139.

[14] CHANG T Y, HAWANG M S, YANG W P. An improvement on the Lin-Wu (t, n)- threshold verifiable multi-secret sharing scheme [J]. Applied Mathematics and Computation, 2012, 170(1): 169 – 178.

[15] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing [J]. SIAM Journal on Computing, 2001, 32(3): 586 – 615.

[16] HORWITZ J, LYNN B. Toward hierarchical identity-based encryption[C]// EUROCRYPT'02: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology. Berlin: Springer-Verlag, 2002: 466 – 481.

(上接第 1385 页)

[7] DENT A W. Hybrid signcryption schemes with outsider security [C]// ISC 2005: Proceedings of the 8th International Conference on Information Security. LNCS 3650. Berlin: Springer-Verlag, 2005: 203 – 217.

[8] LI F, SHIRASE M, TAKAGI T. Identity-based hybrid signcryption [C]// ARES 2009: Proceedings of the Fourth International Conference on Availability, Reliability and Security. Washington, DC: IEEE Computer Society, 2009: 534 – 539.

[9] LI F G, SHIRASE M, TAKAGI T. Certificateless hybrid signcryption [C]// ISPEC 2009: Proceedings of the 5th Information Security Practice and Experience Conference, LNCS 5451. Berlin: Springer-Verlag, 2008: 112 – 123.

[10] SELVI S S D, VIVEK S S, RANGAN C P. Certificateless KEM and hybrid signcryption schemes revisited [C]// ISPEC 2010: Proceedings of the 6th Information Security Practice and Experience, LNCS 6047. Berlin: Springer-Verlag, 2010: 294 – 307.

[11] 孙银霞, 李晖. 高效无证书混合签密[J]. 软件学报, 2011, 22 (7): 1690 – 1698.

[12] 金春花, 李学俊, 魏鹏娟, 等. 新的无证书混合签密[J]. 计算机应用研究, 2011, 28(9): 3527 – 3531.

[13] SINGH K. Identity based hybrid signcryption revisited [C]// ICITeS 2012: Proceedings of the 2012 International Conference on Information Technology and e-Services. Washington, DC: IEEE Computer Society, 2012: 34 – 39.

[14] CAO X, KOU W, DANG L, *et al*. IMBAS: identity-based multi-user broadcast authentication in wireless sensor networks [J]. Computer Communications, 2008, 31(4/5): 659 – 671.

[15] Crossbow technology incorporation . MICA 2 datasheet [EB/OL]. [2012 – 11 – 01]. http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf/.

[16] IEEE. 2.4GHz IEEE 802.15.4/ZigBee-ready RF transceiver [EB/OL]. [2012 – 11 – 01]. http://focus.ti.com/lit/ds/symlink/cc2420.pdf/.

[17] GURA N, PATEL A, WANDER A. Comparing elliptic curve cryptography and RSA on 8-bit CPUs [C]// CHES'04: Proceedings of the Cryptographic Hardware and Embedded Systems. Heidelberg: Springer-Verlag, 2004: 119 – 132.

[18] YASMIN R, RITTER E, WANG G. A pairing-free ID-based one-pass authenticated key establishment protocol for wireless sensor networks [C]// SENSORCOMM 2011: Proceedings of the Fifth International Conference on Sensor Technologies and Applications. Nice, France: IARIA, 2011: 340 – 347.

[19] ISLAM S H, BISWAS G P. A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem [J]. The Journal of Systems and Software, 2011, 84(11): 1892 – 1898.

[20] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing [J]. Journal of Cryptology, 2004, 17(4): 297 – 319.