基于双线性对的秘密分享方案 *

柏钦玺[1], 黄崇超[2], 刘 锋[1]
(1. 鲁东大学 数学与信息学院, 山东 烟台 264025; 2. 武汉大学 数学与统计学院, 武汉 430072)

摘 要: 提出了一种新的基于双线性对的门限秘密分享方案,并对其正确性、安全性和性能进行了分析讨论;该方案将分享者私钥计算和秘密分发过程分离,秘密份额可以重新利用,具有更好的性能,更适合实际应用。

关键词: 秘密分享; 双线性对; 密钥更新
中图分类号: TN918 **文献标志码**: A **文章编号**: 1001-3695(2010)03-1045-02
doi:10.3969/j.issn.1001-3695.2010.03.066

Secret sharing scheme based on bilinear pairings

BAI Qin-xi[1], HUANG Chong-chao[2], LIU Feng[1]
(1. *School of Mathematics & Information, Ludong University, Yantai Shandong* 264025, *China*; 2. *School of Mathematics & Statistics, Wuhan University, Wuhan* 430072, *China*)

Abstract: This paper proposed a new secret sharing scheme based on the bilinear parings. And discussed its correctness, security and performance. At the same time, the proposed scheme departs the private keys of participants computation from the secret distribution process, which made this scheme more secure and more efficient. Therefore, the proposed scheme is more applicable than the existing ones.

Key words: secret sharing; bilinear pairings; key updating

0 引言

秘密分享(secret sharing)是信息安全和数据保密中的一项重要技术,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] 独立提出。基本的秘密分享方案由秘密份额的分配算法和秘密的恢复算法构成。

当前对于秘密分享的研究主要集中在可验证秘密分享、多秘密分享、秘密份额的有效分发、秘密分享的信息率等方面[3],除此之外,基于新的设计思想和数学模型来设计秘密分享方案[4~8]也是一个研究热点。

随着双线性对在公钥密码方面的成功应用,利用双线性变换构造新型的秘密分享方案是一种新的尝试。这种尝试是合理的,因为从广义上看,秘密分享方案也是一个特殊的公钥算法,即由一个秘密分发者加密(加密密钥为秘密分发者私钥),由符合条件的一组秘密分享者解密(解密密钥为分享解密行为的各分享者私钥或称秘密份额)。

鉴于以上考虑,本文在 Shamir 门限秘密分享方案基础上提出一种基于双线性对的秘密分享方案,并分析了此方案的性能。该方案除了能够实现秘密分享系统的基本功能外,相对于现有方案,还具有一些新特性,使得其安全性和效率更好,更适合于实际应用。

1 基础知识

1.1 双线性变换

定义 双线性变换。设$(G_1,+)$和$(G_2,\cdot)$是两个阶为素数 p 的循环群。其中前者为加法群,后者为乘法群。令 g 为 G_1 的生成元。如果满足以下性质,则称变换 $e:G_1\times G_1\to G_2$ 为双线性变换:

a)双线性。对任意 P_1、P_2 和 $Q\in G_1$,有

$$e(P_1+P_2,Q)=e(P_1,Q)e(P_2,Q)$$
$$e(Q,P_1+P_2)=e(Q,P_1)e(Q,P_2)$$

b)非退化性。存在 $g\in G_1$ 即 $e(g,g)\neq 1$,也就是说 $e(g,g)$ 是 G_2 的生成元。

c)可计算性。对任意 P_1、$P_2\in G_1$,存在有效的算法计算 $e(P_1,P_2)$。

1.2 Shamir 秘密分享方案

Shamir 方案由系统初始化、秘密的分发、秘密的恢复三个阶段组成。

1.2.1 系统初始化

秘密分发者 SD 选择如下系统参数:

a)SD 从 Z_p 中选取 n 个不同的非零元 ID_i,并将 ID_i 分配给秘密分享者 $P_i(1\leqslant i\leqslant n)$,作为 P_i 的身份标志符。

收稿日期: 2009-07-01; **修回日期**: 2009-08-24 **基金项目**: 国家自然科学基金资助项目(70771079);鲁东大学人才基金资助项目(LY20062706);鲁东大学科研基金资助项目(L20082702)

作者简介:柏钦玺(1978-),男,山东新泰人,硕士,主要研究方向为系统优化建模与算法、密码学理论及其应用等(baiqinxi98@163.com);黄崇超(1957-),男,湖北公安人,教授,博导,博士,主要研究方向为系统优化建模与算法、信息安全等;刘锋(1980-),男,山东单县人,硕士,主要研究方向为密码学理论及其应用等.

b)SD 在公布栏 NB 中公布信息$\{p,\mathrm{ID}_i\}$。

1.2.2 秘密的分发阶段

1)SD 随机选择一个次数为 $t-1$ 的秘密多项式 $f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}$。

2)SD 为系统每一个秘密分享者 P_i 计算其秘密份额 $x_i=f(\mathrm{ID}_i)$, SD 将参与者的秘密份额 x_i 通过一条安全信道发送给相应的秘密参与者。

1.2.3 秘密的恢复

不失一般性, 若前 t 个参与者合作想要恢复秘密 s,则他们都给出自己相应的身份标志符 ID_i 和秘密分享份额 $x_i(1\leqslant i\leqslant t)$。利用$\{(\mathrm{ID}_i,x_i)\mid i=1,2,\cdots,t\}$ t 个点,以及 Lagrange 插值公式构造如下多项式:

$$f(x)=\sum_{i=1}^{t}f(\mathrm{ID}_i)\prod_{j\neq i}^{t}\frac{x-\mathrm{ID}_j}{\mathrm{ID}_i-\mathrm{ID}_j}=\sum_{i=1}^{t}x_i\prod_{j\neq i}^{t}\frac{x-\mathrm{ID}_j}{\mathrm{ID}_i-\mathrm{ID}_j}$$

从而得到 $s=f(0)=a_0$, 即可恢复秘密 s。

2 双线性对秘密分享方案

设$(G_1,+)$和$(G_2,\cdot)$是两个阶为素数 p 的循环群。其中前者为加法群,后者为乘法群。且满足 G_1 中 Diffie-Hellman 计算问题为困难问题。令 g 为 G_1 的生成元;令 e 为 G_1 和 G_2 上的双线性变换, 即 $e:G_1\times G_1\to G_2$;令 w 为包括 n 个参与者的集合。本文提出的秘密分享方案包括以下三部分。

2.1 系统建立过程

系统建立过程由秘密分发者执行,主要用于建立系统公钥和秘密分发者的私钥。

令 $w=\{P_1,P_2,\cdots,P_n\}$,其中 $\mathrm{ID}_i(i=1,2,\cdots,n)$是 $P_i(1\leqslant i\leqslant n)$的身份标志符,是不等于零的正整数。不同的分享者 P_i 身份标志符 ID_i 互不相同,即 $i\neq j$ 时,$\mathrm{ID}_i\neq\mathrm{ID}_j$。分发者随机地选取 $x\in z_p$ 作为私钥,令 $y=xg$ 为系统的公钥。

2.2 秘密分发过程

为了在这 n 个分享者集合 W 中分享秘密信息 $m\in G_2$,使得至少 t 个分享者合作才可以重构秘密, 秘密分发者可以执行如下过程:

a)分发者随机选择一个次数为 $t-1$ 的秘密多项式$f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}$,为系统每一个秘密分享者 P_i 计算其秘密份额 $x_i=f(\mathrm{ID}_i)$,SD 将分享者的秘密份额 x_i 通过一条安全信道发送给相应的秘密分享者作为私钥。

b)分发者随意选取 $k\in Z_p$ 计算

$$\begin{cases}s=a_0g\\ l=l(kg+xs)a_0^{-1}\\ v=me(g,kg)\end{cases}\tag{1}$$

然后将 s 销毁, 将 l、v 以广播的形式公开。

2.3 秘密重构过程

对于任意阶数为 t 的分享者集合都可以恢复秘密,假设前 t 个分享者合作恢复秘密,将 t 个人的私钥 x_i、ID_i 汇集,通过以下方法可得到

$$m=v\prod_{i=1}^{t}\left[\frac{e(y,x_ig)}{e(x_ig,l)}\right]^{\prod_{j\neq i}^{t}\frac{-\mathrm{ID}_j}{\mathrm{ID}_i-\mathrm{ID}_j}}\tag{2}$$

下面证明式(2)的正确性。

证明 由式(1)知,$e(s,l)=e(a_0g,(kg+xs)a_0^{-1})=e(g,kg+xs)=e(g,kg)e(g,xs)=e(g,kg)e(xg,s)=e(g,kg)e(y,s)$,所以 $e(g,kg)^{-1}=\frac{e(y,s)}{e(s,l)}$。

由式(1)的第一个式子和 Shamir 门限秘密分享方案可知:

$$s=a_0g=\sum_{i=1}^{t}f(\mathrm{ID}_i)\prod_{j\neq i}^{t}\frac{-\mathrm{ID}_i}{\mathrm{ID}_i-\mathrm{ID}_j}g;$$

$$e(g,kg)^{-1}=\frac{e(y,s)}{e(s,l)}=\frac{e\left(y,\sum_{i=1}^{t}f(\mathrm{ID}_i)\prod_{j\neq i}^{t}\frac{-\mathrm{ID}_i}{\mathrm{ID}_i-\mathrm{ID}_j}g\right)}{e\left(\sum_{i=1}^{t}f(\mathrm{ID}_i)\prod_{j\neq i}^{t}\frac{-\mathrm{ID}_i}{\mathrm{ID}_i-\mathrm{ID}_j}g,l\right)}=$$

$$\frac{\prod_{i=1}^{t}e\left(y,f(\mathrm{ID}_i)\prod_{i=1}^{t}\frac{-ID_i}{\mathrm{ID}_i-\mathrm{ID}_j}g\right)}{\prod_{i=1}^{t}e\left(f(\mathrm{ID}_i)\prod_{i=1}^{t}\frac{-\mathrm{ID}_i}{\mathrm{ID}_i-\mathrm{ID}_j}g,l\right)}=$$

$$\left(\prod_{i=1}^{t}\frac{e(y,f(\mathrm{ID}_i)g)}{e(f(\mathrm{ID}_i)g,l)}\right)^{\prod_{i\neq j}^{t}\frac{-\mathrm{ID}_i}{\mathrm{ID}_i-\mathrm{ID}_j}}$$

由式(1)的第三个式子得

$$m=v\cdot e(g,kg)^{-1}=v\cdot\left(\prod_{i=1}^{t}\frac{e(y,f(\mathrm{ID}_i)g)}{e(f(\mathrm{ID}_i)g,l)}\right)^{\prod_{j\neq i}^{t}\frac{-\mathrm{ID}_i}{\mathrm{ID}_i-\mathrm{ID}_j}}$$

由此可见,式(2)正确。

3 安全与性能分析

3.1 安全性

攻击 1 w 中某不良成员 P_j 企图在秘密份额分发的阶段获取 SD 对秘密享有的秘密份额 x。不良成员不可能从公布栏中公布的公钥 $y=xg$ 中计算出 x。因为笔者知道离散对数问题是 NP 完全问题,当 p 是一个大素数时,求解离散对数被认为是不可行的,从而保证了方案的安全性,并且攻击者也不可能从 $l=(kg+xs)a_0^{-1}$,$v=me(g,kg)$ 中计算出 x。

攻击 2 当某个秘密分享者 P_i 的秘密份额 x_i 意外泄露时,秘密分发者只需要重新为秘密分享者选择身份标志符 ID_i(与之前所选取的身份标志符不同),计算新的秘密份额 $x_i=f(\mathrm{ID}_i)$并将其发送给分享者,当然其他分享者的秘密份额无须改变。

3.2 性能分析

本节主要从可行性、秘密份额的重复利用性、成员的增加、存储和通信等方面来分析。

从可行性来看,在秘密恢复阶段,当秘密参与者 P_i 从公告栏 NB 中下载到身份标志 ID_i 后,提供出自己对秘密持有的秘密份额 x_i,然后根据公开的 l、v 和式(2)即可恢复出秘密 m,这样就可以实现秘密的分享。

从秘密份额的重复利用性来看,对于另一个秘密 $m'\in G_2$,由于秘密的恢复与所选取的多项式是独立的,秘密分享者只需修改 l,v 为 l'、v',对于已经分发过的秘密份额 x_i,可以重复利用而无须收回、销毁或修改。该方案秘密可以更新,秘密份额可以重新利用,所以是一个动态的秘密分享方案。

假设有新成员 ID_j 加入到系统中,秘密分发者只需利用多项式计算出新成员的私钥 $x_j=f(\mathrm{ID}_j)$,其他秘密分享者不变动而使得整个方案重新执行。

(下转第 1051 页)

模型的实验仿真环境,并仿真构建实际锅炉工业控制以太网系统检验测试模型的可行性。仿真实验结果表明,该模型能有效定量反映工业控制以太网的可信性能。从掌握的资料分析目前国内有关工业控制网络可信评价的软件系统还是空白,笔者下一步研究的目标是以该模型为基础完善技术细节,通过 Chariot 和 SAS 软件相关 API 函数调用集成开发工业控制网络可信评价软件系统。

参考文献:

[1] 罗军舟,韩志耕,王良民. 一种可信可控的网络体系及协议结构[J]. 计算机学报,2009,32(3):391-404.

[2] 黄晓璐,闵应骅,吴起. 网络流量的半马尔可夫模型[J]. 计算机学报,2009,32(10):1592-1600.

[3] 李沁, 曾庆凯. 一种基于协议分析的可信信道评估方法[J]. 计算机学报,2009,32(8):1299-1366.

[4] 林闯,彭雪海. 一种可信可控的网络体系及协议结构[J]. 计算机学报,2005,28(5):751-758.

[5] 张怡,孙志刚. 面向可信网络研究的虚拟化技术[J]. 计算机学报,2009,32(3):417-423.

[6] Hu S,YAN Wei-yong. Stability of networked control systems: analysis of packet dropping [C]//Proc of International Conference on Control, Automation, Robotics and Vision. 2004: 304-309.

[7] ZHANG Ya , TIAN Yu-ping , CAI Jun. Stability analysis of networked control systems with packet loss [C]//Proc of the 6th World Congress on Control and Automation. 2006: 4556-4560.

[8] LIU Xiang-heng, GOLDSMITH A. Wireless communication tradeoffs in distributed control [C]// Proc of the 42nd IEEE Conference on Decision and Control. 2003: 688-694.

[9] ABADI M,TUTTLE M R . A semantics for a logic of authentication. [C]//Proc of the 10th Annual ACM Symposium on Principles of Distributed Computing . [S. L]:ACM Press,1991: 201-216.

[10] NILSSON J. Real-time control systems with delays [D]. Lund, Sweden: Department of Automatic Control, Lund Institute of Technology, 1998.

[11] LEE K C , LEE S. Remote controller design of networked control system using genetic algorithm[J]. IEEE International Symposium on Industrial Electronics, 2001, 1(3): 1845-1850.

[12] YANG Yue-quan, XU De, TAN Min. Hybrid and stochastic stabilization ana-lysis and H_∞ control for networked control systems [C]// Proc of IEEE Conference on Robotics, Automation and Mechatronics. 2004: 502-506.

[13] PARK H, KIM Y, KIM D, *et al*. A scheduling method for network-based control systems [J]. IEEE Trans on Control Systems Technology, 2002, 10(3): 318-330.

[14] CHAN H, OZGUNER U. Closed-loop control of systems over a communication network with queues [J]. International Journal of Control, 1995, 62(3): 493-510.

[15] ZHANG Wei . Stability analysis of networked control systems [D]. [S.l.]: Case Western Reserve University, 2001.

[16] RAY A, HALEVI Y. Integrated communication and control systems: Part II-design consideration [J]. ASME Journal of Dynamic Systems, Measurement and Control, 1988, 110(4): 374-381.

[17] NILSSON J , BERNHARDSSON B , WITTENMARK B. Stochastic analysis and control of real-time systems with random time delays [J]. Automatica, 1998, 34(1): 57-64.

[18] 薛富波,张文彤,田晓燕. SAS8.2 统计应用教程[M]. 北京:北京希望电子出版社,2004.

(上接第 1046 页)

从存储量来看,系统存储量包括公开信息大小和需要保密的秘密信息大小。对于秘密分发者来说,需要保密的信息仅为私钥 y;对于每个分享者来说,需要保密的信息同样仅为其私钥,其私钥 x_i 长度与所共享秘密 m 的长度相同,不会给系统造成过大的存储负担,因此,本文方案也是一个理想的方案。

从通信性能上来看,除了为分享者计算私钥时需要点对点的单播通信外,其余信息都可以通过广播形式进行传递。众所周知,广播是最有效、最节约能量的通信方式,而本文方案可以有效地利用广播通信方式, 因此具有较好的通信性能。

从实现过程上来看,与现有大多数方案相比,本文方案还有一个特点,就是分享者私钥(或秘密份额)的计算与秘密分发过程是分离的。本文以文献[1]的方案为代表与本文方案作一比较。文献[1]的方案包含三个过程,即系统参数建立、秘密分发和秘密重构过程。其中秘密分发过程融合了分享者私钥的计算。在本文方案中,因为分享者私钥计算可以预处理完成,而在分发秘密时,只需要一次广播即可;而文献[1]的方案事先无法预计算分享者私钥,只能在秘密分发过程中逐一安全发送,所以本文方案秘密分发效率更高。另外,在文献[1]的方案中,只要给分享者分发了私钥,就无法撤销所分享的秘密;而在本文方案中,秘密分发者还有权决定是否要分享某个秘密,因此,本文方案从秘密分发效率和安全性上更适合应用。

4　结束语

本文基于双线性变换构建了一个新的秘密分享方案。该方案将分享者私钥计算与秘密分发过程分离,可以重复利用秘密份额,是一个动态的秘密分享方案。本文方案是一个可证明安全的、有效的秘密分享方案,比现有方案更具安全性和有效性,更适合实际应用。

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. Safeguarding cryptographic key[C]//Proc of AFIPS 1979 National Computer Conference. 1979:313-317.

[3] JEFFERS J, ARAKALA A. Minutiae-based structures for a fuzzy vault[C]//Proc of IEEE Biometrics Symposium. 2006:760-769.

[4] 刘锋,何业锋,程学翰. 动态的(t,n)门限多秘密分享方案[J]. 计算机应用研究, 2008,25(1):240-241.

[5] ASMUTH C, BLOOM J. A modular approach to key safeguarding [J]. IEEE Trans on Information Theory, 1983, 29(2): 208-210.

[6] KARNIN E D, GREENE J W, HELLMAN M E. On sharing secret systems[J]. IEEE Trans on Information Theory, 1983, 29(1): 35-41.

[7] 庞辽军, 王育民. 一个基于几何性质的(t, n)多重秘密共享方案[J]. 西安交通大学学报, 2005, 39(4): 425-428.

[8] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[J]. SIAM Journal of Computation, 2003, 32(3): 586-615.