基于环境感知的防泄漏多秘密共享方案

秦华旺，朱晓华，戴跃伟

(南京理工大学自动化学院 南京 210094)

【摘要】提出了一种基于环境感知的防泄漏多秘密共享方案。在该方案中，可信中心利用中国剩余定理将多个秘密合并成一个秘密，根据拉格朗日插值多项式为各个参与者分配秘密子份额；在秘密重构时，参与者利用双线性映射，根据其秘密子份额和当前环境信息计算伪子份额；验证机构利用拉格朗日插值和双线性映射计算出验证信息，来验证参与者提交的伪子份额的有效性。该方案中参与者的子份额以及共享秘密均具有防泄漏特性，因而可以被重复使用。基于环境感知的动态性可以极大提高该方案对移动攻击者的攻击难度。该方案尤其适用于无线传感器网络、多机器人等野外工作的系统，可以有效提高这些系统的使用效率和安全性。

关 键 词 密码学; 环境感知; 防泄漏; 多秘密共享; 秘密共享
中图分类号 TP393 文献标志码 A doi:10.3969/j.issn.1001-0548.2015.01.017

Leakproof Multi-Secret Sharing Based on Environment Sensing

QIN Hua-wang, ZHU Xiao-hua, and DAI Yue-wei

(School of Automatization, Nanjing University of Science and Technology Nanjing 210094)

Abstract A leakproof multi-secret sharing scheme based on environment sensing is proposed, in which the private key generator (PKG) uses the Chinese remainder theorem to combine multi-secret into one secret, and computes the shadows through the Lagrange interpolation polynomial. In the reconstruction, the participants use the bilinear map to compute the counterfeit shadows according to the shadows and the current environment. The verifier computes the authentication information through the Lagrange interpolation and the bilinear map, and checks the validity of the counterfeit shadows. In the scheme, the shadows of participants and the shared secret are leakproof, and can be used repeatedly. The dynamic property based on environment sensing can improve the security against the mobile adversary. The proposed scheme is particularly suitable for the system which needs to run long time in the open, such as the wireless sensor network and the multi-robots, and can improve the efficiency and security of these systems effectively.

Key words cryptography; environment sensing; leakproof; multi-secret sharing; secret sharing

秘密共享是密码学中的重要研究内容，最早的秘密共享方案由文献[1]提出，其通过拉格朗日插值，实现了(t,n)秘密共享。该方案将秘密分为n个子份额并分发给n个参与者，n个参与者中的任意t个合作可以重构出共享秘密，而少于t个参与者则不能获取有关共享秘密的任何信息。虽然目前已有多种不同形式的秘密共享，如针对访问结构的[2]、可验证的[3-4]、先应式的[5-6]、有权重的[7-8]、多秘密共享的[9-10]等，但这些方案在实际应用中仍然存在以下两点不足：

1) 在共享秘密的重构过程中，秘密生成者会得到原始的共享秘密，因此共享秘密只能被使用一次，而不能被重复使用；2) 参与者不能根据其感知的当前环境来动态改变其提交的子份额或伪子份额，以提高攻击者获取有效子份额的难度。

针对上述问题，本文提出一种基于环境感知的防泄漏多秘密共享方案，该方案中，参与者可以根据其当前感知的环境信息，如时间、温度、湿度、气压等，来动态改变其提交的伪子份额。每次提交的伪子份额均有一定的有效期，超出有效期的伪子份额将不可用，即使攻击者获取了某个授权子集中全部参与者的过期伪子份额，攻击者也不能获取共享秘密的任何信息，由此可以极大提高攻击者的攻击难度。在重构共享秘密的过程中，不论是各个参与者、秘密生成者还是共享秘密的验证机构，均不能直接获取原始的共享秘密，而只能由可信的验证机构对秘密生成者提供的关于共享秘密的验证信息

收稿日期：2013 – 12 – 12；修回日期： 2014 – 09 – 10
基金项目：国家自然科学基金(61170250, 61103201)
作者简介：秦华旺(1978 –)，男，博士，副教授，主要从事信息安全方面的研究.

进行有效性验证，因此共享秘密可以被重复使用，从而有效提高系统的使用效率。此外，本文方案还利用中国剩余定理实现了多秘密共享。与传统的先应式秘密共享方案相比，本文方案不需要通过参与者间大量的信息交互进行子份额更新，因而也就不需要在参与者间采用复杂的数据同步和交互协议，可以极大降低系统设计的复杂度，并提高系统运行的鲁棒性。

本文提出的基于环境感知的防泄漏多秘密共享方案在实际中具有重要的应用价值，如在野外的无线传感器网络、多机器人等系统中，通常在投放前对系统进行共享秘密分发，这些节点将在野外长期工作，如果此时再对系统进行共享秘密的分发将极其麻烦。因此，如果系统的共享秘密，或者参与者的子份额只能被使用一次，而不能被重复使用，将严重影响系统的工作效率。使用本文提出的基于环境感知的防泄漏秘密共享方案，无线传感器或机器人可通过感知的环境信息动态更新其提交的伪子份额，提高攻击者同时获取多个有效伪子份额的难度，并使原始的共享秘密在重构过程中不被泄漏，可以被重复使用，极大提高了系统的使用效率和安全性。此外，在基于互联网的秘密共享系统中，共享秘密的分发也是一件繁琐的工作，需要采用高可靠性的加密措施或维护一些高安全性的秘密通道。在这类系统中使用本文提出的基于环境感知的防泄漏秘密共享方案，同样将有效提高系统的使用性能。

1 相关工作

(t,n)门限秘密共享方案最早由文献[1,11]提出，规定n个参与者中的任意t个合作可以重构出共享秘密。文献[1]方案基于拉格朗日插值，而文献[11]的方案则基于共点超平面。为了拓宽秘密共享的应用范围，文献[2]又提出了访问结构上的秘密共享方案，在该方案中，参与者集合可以划分为若干个数量不等的授权子集，并规定只有授权子集中的参与者合作才能得到共享秘密。此外，针对实际中可能出现的各个参与者重要程度不同的应用需求，又出现了参与者有权重的秘密共享方案[7-8]，这些方案的构造，可以在(t,n)秘密共享的基础上通过给权重不同的参与者分配数量不同的子份额实现[7]，也可以通过采用分解结构[8]实现。

除了门限结构外，秘密共享在其他方面也取得了丰富的研究成果。比较典型的有文献[3-4]的可验证秘密共享，可以对参与者在秘密重构中提交的子份额进行公开验证，以防止参与者的欺骗行为。文献[5]的先应式秘密共享通过周期性更新各个参与者的子份额，提高方案对移动攻击的防御能力。文献[6]的动态先应式秘密共享在更新子份额时还可以改变秘密共享的门限结构，从而提高了方案在应用中的灵活性。文献[9]的多秘密共享只需要一次分发，就可以同时共享多个秘密。文献[12]的无可信中心的秘密共享中的各个参与者同时也是秘密的分发者，可以避免系统的单点失效问题。

近期还有其他一些新颖的秘密共享方案被提出，如文献[13]的分级秘密共享，可以将整个参与者集合分成若干个等级，不同级别的门限值也不同。文献[14]的空间高效秘密共享，利用多重的多项式插值，使各个参与者只需保存接近于理论上最小长度的子份额。文献[15]的可纠错秘密共享假设共享秘密的子份额受到了噪声的干扰，给出了在此情况下可以重构出共享秘密的条件，并设计了相应的可纠错的秘密共享方案。文献[16]的社会秘密共享根据参与者的声誉以及其在秘密共享中表现出的可靠性来为其分配子份额。

在现有秘密共享方案中，共享秘密在重构过程中均会被暴露，使其不能被重复使用，影响了系统的使用效率，而且参与者也不能根据当前环境动态改变其提交的子份额或伪子份额，只能基于复杂通信协议基础上的大量信息交互来更新子份额，提高了系统设计的复杂性。针对该问题，本文提出基于环境感知的防泄漏多秘密共享方案，与现有方案相比，本文方案的主要优点有：

1) 共享秘密在重构过程中不会被泄漏，因此其可以被重复使用；2) 参与者可以根据当前感知的环境信息来动态改变其提交的伪子份额，伪子份额具有一定的有效期，过期的伪子份额不能用于重构共享秘密；3) 能够实现多秘密共享，各个秘密可以具有不同的门限值。

2 双线性映射

令G_1是q阶加法群，G_2是q阶乘法群，q是大素数，若映射e：$G_1\times G_1\to G_2$满足下列条件，则e就被称为双线性映射[17]。

1) 双线性：对于所有的P，$Q\in G_1$和$a,b\in Z_q$，有$e(aP,bQ)=e(P,Q)^{ab}$。2) 非退化性：存在$P,Q\in G_1$，使得$e(P,Q)\neq 1$。3) 可计算性：对于任意的$P,Q\in G_1$，存在有效的算法来计算$e(P,Q)\in G_2$。

双线性映射中的困难性问题是利用双线性映射

来设计密码系统的基础，本文方案将用到一个被称为“计算性Diffie-Hillman问题(CDH)”的困难问题。即：对于给定的参数$P,aP,bP,cP\in G_1$，其中$a,b,c\in Z_q$未知，计算$e(P,P)^{abc}$。可以认为不存在能以不可忽略的概率优势解决CDH问题的多项式时间算法。

3　方案描述

在基于环境感知的防泄漏秘密共享方案中，参与者重构的并不是原始的共享秘密，而只能重构共享秘密有效的验证信息，该验证信息需要一个可信的专门验证机构进行验证。同样，验证机构也不可以获取原始的共享秘密。

各个参与者以及验证机构均可以通过传感器感知当前的环境信息，包括时间、温度、湿度、气压等。本文方案中，所有节点感知的环境信息必须一致。因此，如果参与者以及验证机构的分布范围较小，如一个小范围的多机器人系统，则时间、温度、湿度、气压等环境信息均可以利用。如果参与者以及验证机构的分布范围较大，温度、湿度、气压等环境信息则无法保证一致性，此时可以利用时间信息，因为在全球范围内通过GPS感知的时间信息均可以保证高度的一致性。鉴于时间信息在精度、同步性、不重复性等方面具有的优势，本文方案中的环境信息将以时间为例。

通过GPS可以获取精度非常高的时间值，系统根据共享秘密重构过程所需要的时间选择合适的时间单位。为了保证参与者以及验证机构获取时间的一致性，由验证机构在某个时间单位的开始时广播通知所有参与者获取当前时间。若秘密重构及验证在1 min内完成，则验证机构可以在开始时通知所有参与者获取时间，且获取的时间单位定为min。在整个重构及验证过程中，所有参与者和验证机构所保存的时间值一致，且所有参与者提交的伪子份额的有效期均为1 min，超出1 min的伪子份额将无效。通过给参与者的伪子份额加上有效期，能极大提高攻击者的攻击难度。

3.1　初始化

令$U=\{u_1,u_2,\cdots,u_n\}$代表n个参与者的集合，$K_1,K_2,\cdots,K_m$为需要共享的m个秘密，门限值分别为$t_1,t_2,\cdots,t_m$，设$t_1\le t_2\le\cdots\le t_m$。本文采用文献[10]的方法，利用中国剩余定理将多个共享秘密合成为一个秘密。为了实现基于环境感知的防泄漏多秘密共享，可信中心PKG首先需要进行一些初始化操作。

1) 可信中心PKG选择一个双线性映射e：$G_1\times G_1\to G_2$，G_1的阶为大素数q，生成元为P。2) PKG选择一个Hash函数H(·): $\{0,1\}^*\to G_1$。3) PKG选择m个互不相同的素数$p_1<p_2<\cdots<p_m$，且$K_i<p_i$，$i=1,2,\cdots,m$。4) PKG公开$(e,G_1,G_2,q,P,\mathrm{H}(),p_1,p_2,\cdots,p_m)$。5) PKG随机选取$s\in Z_q^*$作为验证机构的私钥，计算验证机构的公钥$Q=sP$并公开。6) PKG随机选取$x_1,x_2,\cdots,x_n\in Z_q^*$作为$n$个参与者的私钥，计算各个参与者的公钥$U_i=x_iP$并公开。7) PKG利用安全通道将$x_i\,(i=1,2,\cdots,n)$秘密发送给参与者$u_i$，将$s,K_1P,K_2P,\cdots,K_mP$秘密发送给验证机构。

3.2　子份额分发

1) PKG建立如下的方程组，利用中国剩余定理将$K_1,K_2,\cdots,K_m$合并成一个秘密K。

$$\begin{aligned}K&\equiv K_1 \bmod p_1\\K&\equiv K_2 \bmod p_2\\&\vdots\\K&\equiv K_m \bmod p_m\end{aligned}$$

2) PKG任意选择t_1-1个整数$a_1,a_2,\cdots,a_{t_1-1}\in Z_M$，其中，$M=\prod_{i=1}^{m}p_i$。计算系数$a_{t_i},a_{t_i}+1,\cdots,a_{t_{i+1}}-1$，方法为：$a_j\equiv b_jr_j\prod_{k=1}^{i}p_k \bmod M$，$j=t_i,t_i+1,\cdots,t_{i+1}-1$，$i=1,2,\cdots,m-1$，其中，$b_j$从$\{0,1,\cdots,p_i-1\}$中任意选择，$r_j$为任意整数。

3) PKG建立方程$f(x)=K+\sum_{i=1}^{t_m-1}a_ix^i$。

4) PKG计算$y_i=f(i) \bmod M$，$i=1,2,\cdots,n$，并将y_i作为参与者u_i的子份额，然后利用安全通道将子份额秘密发送给各个参与者。

3.3　重构和验证

设t_j个参与者要重构共享秘密K_j的验证信息，为了便于描述，假设t_j个参与者为$u_1,u_2,\cdots,u_{t_j}$，重构过程如下：

1) 参与者给验证机构发送一个重构消息，然后验证机构在合适的时间点广播通知该t_j个参与者，以一定的时间单位来获取时间值；2) 参与者u_i利用其子份额y_i计算对应于共享秘密K_j的子份额$y_{ij}=y_i \bmod p_j$；3) 设T为验证机构及参与者通过GPS获取的当前时间，参与者u_i首先计算$X_i=x_iQ$，然后再计算其伪子份额$\delta_{ij}=e(P,P)^{y_{ij}\mathrm{H}(T\|X_i)}$，并将$\delta_{ij}$发送给验证机构；4) 验证机构收到$\delta_{ij}$后，先利用Diffie-Hillman密钥交换技术[18]计算$X_i=sU_i$，再计

算 $w_{ij}=\delta_{ij}^{(H(T\|X_i))^{-1} \bmod q}=e(P,P)^{y_{ij}}$，最后计算共享秘密 K_j 的验证信息 $V_j=\prod_{i=1}^{t_j} w_{ij}^{L_i^0} \ (\bmod e(P,P)^{p_j})=e(P,P)^{K_j}$，其中，$L_i^0=\prod_{1\le k\le t_j,k\ne i} -k/(i-k)$。

验证机构通过计算 $V_j=e(K_jP,P)$ 验证参与者提供的验证信息的有效性。

4 性能分析

4.1 有效性

由文献[10]可知，t_j 个子份额 y_{ij} 通过拉格朗日插值可以恢复多项式 $f_j(x)\equiv f(x) \bmod p_j$，且 $f_j(0)=K_j \bmod p_j$，因此，有：

$$V_j=\prod_{i=1}^{t_j} w_{ij}^{L_i^0} \ (\bmod e(P,P)^{p_j})=$$

$$\prod_{i=1}^{t_j} e(P,P)^{y_{ij}L_i^0} \ (\bmod e(P,P)^{p_j})=$$

$$e(P,P)^{\sum_{i=1}^{t_j} y_{ij}L_i^0} \ (\bmod e(P,P)^{p_j})$$

由拉格朗日插值可知，$\sum_{i=1}^{t_j} y_{ij}L_i^0=f_j(0)$，所以 $V_j=e(P,P)^{f_j(0)} \ (\bmod e(P,P)^{p_j})=e(P,P)^{K_j}$。因此，验证机构可以通过计算 $V_j=e(K_jP,P)=e(P,P)^{K_j}$ 验证 V_j 的有效性。

4.2 防泄漏性

参与者在秘密重构时提交的是伪子份额 $\delta_{ij}=e(P,P)^{y_{ij}H(T\|X_i)}$，由计算性Diffie-Hillman问题(CDH)可知，攻击者不能通过 δ_{ij} 推导出 y_{ij}，也无法获取参与者的子份额 y_i。同样，从秘密生成者提交的验证信息 $V_j=e(P,P)^{K_j}$ 中，攻击者也得不到共享秘密 K_j。因此，在整个秘密重构过程中，参与者的秘密子份额和原始的共享秘密都没有被泄漏，可以被重复使用。此外，验证机构也无法通过其保存的 K_jP 来获取 K_j。

4.3 基于环境感知的动态性

在秘密重构时，参与者提交的伪子份额 $\delta_{ij}=e(P,P)^{y_{ij}\mathrm{H}(T\|X_i)}$ 中含有当前的时间信息，时间不同，参与者提交的伪子份额也不同，因此伪子份额具有一定的有效期。只有在有效期内的伪子份额才能重构有效的验证信息，过期的伪子份额没有价值，攻击者必须在有效期内获取授权子集中所有参与者提交的伪子份额，才能重构有效的验证信息，这将极大提高攻击者的攻击难度。

5 性能比较

文献[3]的可验证秘密共享和文献[5]的先应式秘密共享，与本文方案的防泄漏、环境感知、可验证等特性较为相似，表1给出了本文方案与文献[3,5]方案之间的性能比较。可以看出，在文献[3,5]的方案中，参与者在秘密重构时提交的是秘密子份额，不能通过提交伪子份额来防止其秘密子份额的泄漏，而本文方案则可以通过提交伪子份额防止秘密子份额的泄漏。

表1 性能比较

性能	方案		
	文献[3]	文献[5]	本文
子份额防泄漏	否	否	是
子份额或伪子份额可更新	否	是	是
共享秘密可重用	否	否	是
计算复杂度	模指数	模指数	模指数
可实现多秘密共享	否	否	是

文献[3]的方案不能进行子份额更新，文献[5]的先应式秘密共享方案可以进行子份额的定期更新，本文方案可以根据当前环境对伪子份额进行动态更新。文献[3]的先应式秘密共享方案通过各个参与者间大量的信息交互，周期性地更新各个参与者的子秘密，增加攻击者同时获取或破坏多个子秘密的难度。但先应式秘密共享需要在各个参与者间进行大量的信息交互，为了保证交互信息的同步和一致性，需要采用复杂的通信协议，增加了系统设计的复杂性。此外，如果攻击者破坏了交互信息中的任何部分，将导致整个门限密码系统失效，因此文献[5]的先应式秘密共享方案的鲁棒性也难以得到保证。本文方案不需要在参与者间进行大量的信息交互，因而也就不需要在参与者间采用复杂的数据同步和交互协议，可以极大降低系统设计的复杂度。

本文方案中，达到门限要求的参与者只能重构共享秘密的有效验证信息，不论是各个参与者、秘密生成者还是共享秘密的验证机构，均不能直接获取原始的共享秘密，因此共享秘密可以被重复使用，而现有秘密共享方案则不具备这个特性。

文献[3,5]的方案以及本文方案中的主要计算开销均是模指数运算，因此它们的计算复杂度相当。此外，本文方案可以实现多秘密共享，而文献[3,5]的方案只能进行单秘密共享。

6 结 束 语

秘密共享是保证数据保密性和完整性的一种重要手段，也是密码学和分布式计算领域中的重要研究内容。本文提出了一种基于环境感知的防泄漏多秘密共享方案。与现有方案相比，本文方案的显著特点是共享秘密以及参与者的子份额均具有防泄漏特性，可以被重复使用。此外，其基于环境感知的动态性使参与者提交的伪子份额具有一定的有效期，有效提高攻击者的攻击难度。本文方案尤其适用于野外的无线传感器网络、多机器人等系统中的秘密共享，基于环境感知的防泄漏特性将可以极大提高这些系统的使用效率和安全性。

参 考 文 献

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

[2] ITO M, SAITO A, NISHIZEKI T. Secret sharing schemes realizing general access structure[C]//Proceedings of IEEE Global Telecommunication Conference. New Jersey: IEEE Press, 1987.

[3] FELDMAN P. A practical scheme for non-interactive verifiable secret sharing[C]//Proceedings of the 19th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1987: 427-437.

[4] PEDERSEN T P. Non-interactive and information-theoretic secure verifiable secret sharing[C]//CRYPTO'91, LNCS 576. Berlin: Springer-Verlag, 1992: 11-15.

[5] HERZBERG A, JARECKI S, KRAWCZYK H, et al. Proactive secret sharing or how to cope with perpetual leakage[C]//Cryptology-Crypto'95. Berlin: Springer-Verlag, 1995: 339-352.

[6] DESMEDT Y, JAJODIA S. Redistributing secret shares to new access structures and its applications[C]//Technical Report ISSE TR-97-01. Fairfax, USA: [s.n.], 1997.

[7] MORILLO P, PADRO C, SAEZ G, et al. Weighted threshold secret sharing schemes[J]. Information Processing Letters, 1999, 70: 211-216.

[8] SUN H M, CHEN B L. Weighted decomposition construction for perfect secret sharing schemes[J]. Computers and Mathematics with Applications, 2002,43: 877-887.

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

[10] CHAN C W, CHANG C C. A scheme for threshold multi-secret sharing[J]. Applied Mathematics and Computation, 2005(166): 1-14.

[11] BLAKLEY G R. Safeguarding cryptographic keys [C]//Proceedings of AFIPS National Computer Conference. New York: IEEE Press, 1979: 313-317.

[12] PEDERSEN T P. A threshold cryptosystem without a trusted party[C]//Eurocrypt'91, LNCS 547. Berlin: Springer-Verlag, 1991: 522-526.

[13] TASSA T. Hierarchical threshold secret sharing[J]. Journal of Cryptology, 2007, 20: 237-264.

[14] PARAKH A, KAK S. Space efficient secret sharing for implicit data security[J]. Information Sciences, 2011, 181: 335-341.

[15] KUROSAWA K. General error decodable secret sharing scheme and its application[J]. IEEE Transactions on Information Theory, 2011, 57(9): 6304-6309.

[16] NOJOUMIAN M, STINSON D R, GRAINGER M. Unconditionally secure social secret sharing scheme[J]. IET Information Security, 2010, 4(4): 202-211.

[17] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[C]//ASIACRYPT'01, LNCS 2248. Berlin: Springer-Verlag, 2001: 514-532.

[18] DIFFIE W, HELLMAN M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

编 辑 漆 蓉