基于GDH群可证安全的门限签名方案*)

彭长根[1,2] 张晓培[1] 李 祥[1] 罗文俊[1]

(贵州大学计算机软件与理论研究所 贵阳 550025)[1] (贵州大学理学院数学系 贵阳 550025)[2]

摘 要 分析了Boneh等人的短签名方案和Boldyreva门限签名方案因不具备概率签名特性而可能存在的一种对比攻击;然后基于Gap Diffie-Hellman(GDH)群设计了一个概率型的门限签名方案,并在随机预言模型(Random Oracle Model)下证明了方案的安全性。所提出的方案可以避免对比攻击的风险,并且其安全性不低于Boldyreva方案的安全性,即提供了健壮性和在选择消息攻击下的不可伪造性,并能容忍 $t<n/2$ 个恶意用户的勾结。本文的方案可作为Boldyreva方案的改进。

关键词 门限签名,概率签名,双线性对,GDH群,椭圆曲线密码体制

A Provable Secure Threshold Signature Scheme Based on GDH Group

PENG Chang-Gen[1,2] ZHANG Xiao-Pei[1] LI Xiang[1] LUO Wen-Jun[1]

(Institute of Computer Science, Guizhou University, Guiyang 550025)[1] (Department of Mathematics, Guizhou University, Guiyang 550025)[2]

Abstract There exist the possibility of comparison attacks on the Boneh et al.'s short signature and the Boldyreva's threshold signature due to their schemes couldn't provide the property of probabilistic signature. This paper firstly gives its analysis. Then a threshold signature scheme with the property of probabilistic signature based on the Gap Diffie-Hellman (GDH) group is proposed and its security proof is given in the Random Oracle model. Our construction can prevent the risk of comparison attacks and the security is the same as Boldyreva's threshold signature scheme, that is, it can provide the robustness and unforgeability, and it can tolerate $t<n/2$ malicious parties. The proposed threshold signature scheme can be regarded as the improvement of Boldyreva's constructions.

Keywords Threshold signature, Probabilistic signature, Bilinear pairings, GDH group, Elliptic curve cryptosystem

1 引言

2001年,Boneh等人[1]在Asiacrypt会上提出了一种新的基于双线性对的签名方案,称为短签名方案,并且证明了该方案在随机预言模型(Random Oracle Model)下,能够抵御利用选择消息进行存在性伪造攻击。Boneh等人的短签名方案具有签名长度短、计算效率和通信效率高的优点。但该短签名方案不是一种概率签名体制,为此钱海峰和曹珍富等在文[2]提出了一个改进方案,此方案在不降低安全性的情况下,增加了概率签名的特性,使其对同一消息 m 的重复签名可以得到不同的签名,避免了攻击者通过收集存储若干签名 (m_i,σ_i) 后进行攻击。

门限签名是秘密共享技术和数字签名技术相结合的一种密码体制,是面向群体密码学研究的一个热点,研究成果较多。Boldyreva[3]在2003年提出的基于*GDH*签名的门限签名方案,以其具有通信量和计算量小的特点比较引人注目,该门限签名方案被证明在随机预言模型下能够抵御利用选择消息进行存在性伪造攻击,并且能容忍 t<n/2 个恶意用户。但是由于*GDH*签名不具有概率签名的特性,因此Boldyreva的方案也不是一种概率型的门限签名方案,每次对同一消息的签名结果是一样的,攻击者可以通过收集和存储若干历史签名后实施对比攻击可能导致签名钥的暴露,而且一旦签名钥泄露,对系统的影响会比概率签名体制更大。

本文首先分析了Boneh等人的短签名方案和Boldyreva的门限签名方案存在的对比攻击问题,然后以文[2]的签名方案作为基础签名方案设计了一个门限签名方案,该方案克服了Boldyreva方案因不具有概率签名特性而易受对比攻击的弱点。在随机预言模型下,证明了所设计的方案具有健壮性和不可伪造性,而且也能容忍 $t<n/2$ 个恶意用户。本文的方案是基于*Gap Diffie-Hellman*(*GDH*)群和椭圆曲线密码体制设计,它可以被看作是Boldyreva方案的改进。

2 准备知识及相关方案分析

2.1 双线性对及几个密码学问题

设 G_1 和 G_2 分别为具有阶 q 的循环加法群和循环乘法群,其中 $q\geqslant 2^k$,k 为安全参数。另设 P 为 G_1 的生成元,O 为 G_1 的单位元。双线性对是指满足如下条件的映射 $e:G_1\times G_1\rightarrow G_2$:

1. 双线性:$\forall P,Q\in G_1$ 和 $a,b\in Z_q^*$,有 $e(aP,bQ)=e(P,Q)^{ab}$。

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

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

这样的双线性对可以用超椭圆曲线上经改造的Weil配对或Tate配对构造。以下是与双线性对有关的几个密码学

*)基金项目:国家自然科学基金资助项目(60463001)。贵州省自然科学基金(编号:20052107)和贵州省省长基金(编号:2005368)。彭长根 教授,博士,研究方向为密码学与信息安全;张晓培 讲师,博士研究生,研究方向为安全协议分析;李 祥 教授,博士生导师,研究方向为可计算性理论、密码学与信息安全;罗文俊 教授,博士,研究方向为密码学与信息安全。

问题：

计算 Diffie-Hellman (CDH)问题：给定(P,aP,bP)和未知的$a,b\in Z_q$，计算$abP\in G_1$。

决策 Diffie-Hellman (DDH)问题：给定(P,aP,bP,cP)和未知的$a,b,c\in Z_q$，判断等式$ab=c$是否成立。

若群 G 上的 DDH 问题容易而 CDH 问题困难时，则称群 G 为 Gap Diffie-Hellman(GDH)群。

2.2 Boneh 短签名方案和改进的概率短签名方案

Boneh 等人[1]的短签名方案(简称 GDH 签名)的参数为G_1、G_2、e、P、q、H。其中G_1、G_2、e、P和q为 2.1 节定义的参数，并且G_1为 GDH 群，$H:\{0,1\}^*\rightarrow G_1^*$为安全的 hash 函数。令$cp=(G_1,G_2,P,q,H,e)$为公共参数，该方案由三个算法$GS=(K,S,V)$构成：

密钥生成算法$K(cp)$：随机选取$x\in_R Z_q^*$作为私钥，计算公钥$Y=xP$。

签名算法$S(cp,x,m)$：给定消息$m\in\{0,1\}^*$，计算m的签名$\sigma=xH(m)$。

验证算法$V(cp,Y,m,\sigma)$：给定消息m的签名σ，验证等式$e(P,\sigma)=e(Y,H(m))$是否成立，若等式成立，签名有效。

考虑到 GDH 签名不是一种概率型的签名体制，文[2]对其进行了改进，形成了一种概率签名方案(简称 QCXS 方案)，方案的公共参数为$cp=(G_1,G_2,P,q,H_1,H_2,e)$，参数$G_1,G_2,q,P,e$与短签名方案相同，$H_1:\{0,1\}^*\times G_1\rightarrow Z_q^*$和$H_2:\{0,1\}^*\rightarrow G_1^*$为两个安全的*hash*函数。该方案由三个算法构成，记为$QCXS=(K,S,V)$：

密钥生成算法$K(cp)$：与 GDH 签名方案相同。

签名算法$S(cp,x,m)$：给定消息$m\in\{0,1\}^*$，随机选取$r\in_R Z_q^*$，计算$R=rP$。令$h=H_1(m,R)$，$Q=H_2(m)$，计算$S=(r+hx)Q$，则m的签名为$\sigma=(R,S)$。

验证算法$V(cp,Y,m,\sigma)$：计算$h=H_1(m,R)$，验证等式$e(P,S)=e(R+hY,H_2(m))$是否成立，若等式成立，签名有效。

文[2]还证明了上述的 QCXS 方案的安全性不低于 GDH 签名方案的安全性，即在随机预言模型中，该方案具有在选择消息攻击下的不可伪造性。

2.3 Boneh 短签名方案和 Boldyreva 门限签名方案分析

由于 GDH 签名过程没有采用秘密选取的随机数，从而每次对同一消息的签名结果是一样的，这样就存在对比攻击：$\sigma_i=x_iH(m)$，$\sigma_j=x_jH(m)$，若$\sigma_i=\sigma_j\Rightarrow x_i=x_j$。假设用户$i$的签名钥$x_i$已暴露，敌手就有可能通过比较有关历史签名获得用户$j$的签名钥$x_j$；或者敌手也可以有意识地选择消息通过访问签名模型进行这种攻击。总而言之，敌手存在从存储的签名对(m_i,σ_i)进行对比攻击的机会。

在 Boldyreva[3]基于 GDH 签名所提出的门限签名方案中，签名用户集 R 生成的门限签名为$\sigma=\prod_{i\in R}\sigma_i^{L_i}=\prod_{i\in R}(H(m))^{x_iL_i}=H(m)^x$，其中$L_i$为 Lagrange 系数。由于个体签名$\sigma_i$是用 GDH 签名方法生成的，自然也存在对比攻击，攻击者通过与存储的历史签名和已暴露的签名钥进行比对，就有机会获得签名组的私钥x。

当然上述的对比攻击不一定肯定能成功，但毕竟是一种弱点，因此增加签名的概率特性可以避免这种攻击。

3 基于 GDH 群的$(t+1,n)$门限签名方案

自 Shamir 提出第一个门限秘密共享方案[4]之后，门限密码体制成为了一个研究热点。随后 Pedersen 又提出一个无需可信中心的可验证秘密共享方案[5]，在该方案中，每个成员充当着一个可信中心，但 Gennaro 等人在文[6]中指出 Pedersen 方案存在缺陷，并结合 Feldman 方案[7]和 Pedersen 方案的思想提出了一个分布式密钥分配算法(这里简称为 GJKR 算法)，本节将基于 GJKR 算法进行密钥分配。本节基于 QCXS 方案所提出$(t+1,n)$的门限签名方案(简称 NTS 方案)，主要目的是为了将 Boldyreva 的门限签名方案改进为一种具有概率特性的门限签名方案，该门限方案不需要可信中心。

3.1 方案描述

令$\Omega=\{P_1,P_2,\cdots,P_n\}$为$n$个签名用户，所有用户都连接一个广播信道和一个点对点信道。Ω中的$t+1$个成员(或多于$t+1$个成员)可以实现门限签名，假设这些成员集合记为$\Gamma=\{P_i\}_{i\in\Phi}$，这里$\Phi\subset\{1,2,\cdots,n\}$且$|\Phi|=t+1$，$t$为门限值。本方案的公共参数$cp$与 QCXS 方案的相同。规定在开始签名时，$\Gamma$中用户都被标记为合格。该$(t+1,n)$门限方案由三个算法$NTS=(TK,TS,TV)$构成：

分布式密钥生成算法$TK(cp,x,t,n)$：本算法采用 GJKR 算法实现，该方案不需要可信中心。GJKR 算法是基于离散对数问题(DLP)实现的，显然很容易将其修改为基于椭圆曲线离散对数问题(ECDLP)的分布式密钥分配方案。TK 算法的功能是组$\Omega=\{P_1,P_2,\cdots,P_n\}$中的每个用户运行 GJKR 算法获得组签名钥的共享值，其中P_i获得的共享值为$x_i(i=1,2,\cdots,n)$；然后每个用户P_i计算公钥$Y_i=x_iP$并公开。事实上，发送方的组私钥x可由$(x_1,x_2,\cdots,x_n)\xrightarrow{(t+1,n)}x$获得，相应组公钥为$Y=xP$。

门限签名算法$TS(cp,\Gamma,x_i,m)$：输入共公参数cp、参与签名组Γ及相应成员的私钥x_i和待签名的消息$m\in\{0,1\}^*$，算法执行以下步骤完成门限签名：

(1)$P_i\in\Gamma$随机选取$r_i\in_R Z_q^*$，计算并广播$U_i=r_iP$。

(2)$P_i\in\Gamma$计算$U=\sum_{i\in\Phi}L_iU_i$，$h=H_1(m,U)$，$Q=H_2(m)$$V_i=(r_i+hx_i)Q$，其中$L_i=\prod_{j\in\Phi,j\neq i}\frac{-j}{i-j}$为 Lagrange 系数。

(3)任意从组Γ中指定一个签名用户 D 验证等式

$$e(P,V_i)=e(U_i+hY_i,H_2(m)) \tag{1}$$

是否成立，若等式不成立，则用户P_i被标记为不合格并重新选择签名用户。若Γ中所有用户的部分签名(U_i,V_i)都满足等式(2)，则D计算$V=\sum_{i\in\Phi}L_iV_i$，消息m的门限签名为$\sigma=(U,V)$。

验证算法$TV(cp,Y_i,m,\sigma)$：验证者收到签名(m,σ)后，可以利用公开信息$(Y_1,Y_2,\cdots,Y_n)$对其进行验证。先计算$h=H_1(m,U)$，$Y=\sum_{i\in\Phi}Y_i$，然后验证等式$e(P,V)=e(U+hY,H_2(m))$是否成立，若等式成立，则签名σ有效。

3.2 方案的正确性证明

TS 算法的验证等式(1)的证明：

$$\begin{aligned}e(P,S_i)&=e(P,(r_i+h_ix_i)Q)=e((r_i+h_ix_i)P,Q)\\&=e(R_i+hY_i,H(m))\end{aligned}$$

TV算法中的验证公式也能正确验证门限签名的有效性，因为如果每个签名用户能严格执行签名步骤，则有：

$$\begin{aligned}e(P,V)&=e(P,\textstyle\sum_{i\in\Phi}L_iV_i)=e(P,\sum_{i\in\Phi}L_i(r_i+hx_i)Q)=\\&e(\textstyle\sum_{i\in\Phi}L_i(r_i+hx_i)P,Q)=e(\sum_{i\in\Phi}L_iU_i+\\&hx_iL_iP,Q)=e(\textstyle\sum_{i\in\Phi}L_iU_i+(\sum_{i\in\Phi}x_iL_i)hP,\\&Q)=e(U+hY,H_2(m))\end{aligned}$$

(下转第 148 页)

特别是对于运行元数据密集型应用的集群系统来说至关重要。在客户端设立元数据缓存，经过测试，在缓存命中情况下各操作都有性能提升，有的甚至出现几倍乃至十倍以上的提高。由于元数据缓存块很小决定了几兆容量的内存就能保证极高的命中率，很少有置换情况发生，采用基于 hash 的 LFU-DA 算法改善了元数据缓存查找性能。

参 考 文 献

1 Ousterhout Jk, Costa H D, Harrison D, Kunze J A, Kupfer M, Thompson J G. A tracedriven analysis of the Unix 4. 2 SD file system. In: Proc. eedings of the 10th ACM Symposium on Operating Systems Principles(SOSP'85), Dec. 1985. 15～24

2 Roselli D, Lorch J, Anderson T. A compare-ison of file system workloads. In: Proceedings of the 2000 USENIX Annual Technical Conference, June 2000. 41～54

3 Morris J H, Satyanarayanan M, Conner M H, et al. Andrew: A Distriuted Personal Computing Enviro-nment. Communications of the ACM, 1986, 29(3): 184～201

4 Corett P F, Feitelso D G. The Vesta Parallel File System. ACM Transactions on Computer Systems, 1996, 14(3): 225～264

5 Brandt S A, Xue Lan, Miller E L, et al. Efficient Metadata Management in Large Distriuted File System. In: Proceedings of the 20th IEEE 11th NASA Goddard Conference on Mass Storage Systems and Technologies, 2003(4): 290～298

6 Yan Jie, Zhu Yaolong, Xiong Hui. A Design of Meta data Server Cluster in Large Distriuted Oject-based Storage. In: 12th NASA Goddard, 21st IEEE Conference on Mass Storage Systems and Technologies, 2004(4): 13～16

(上接第 111 页)

3.3 方案的安全性证明

定理 1 即使在一个 PPT 敌手勾结了 $t(t<n/2)$ 个签名用户的情况下，所提出的门限签名方案 NTS 也是安全的，即 NTS 方案具有健壮性。

证明：NTS 方案的 TK 算法是采用 GJKR 算法实现的，Gennaro 等人已在文[6]中证明了在敌手勾结用户数 $t<n/2$ 的情况下，GJKR 算法能成功运行，则 TK 算法也能成功运行。对于 TS 算法，由于部分签名的有效性可以通过(2)式进行验证，即使敌手勾结了 $t(t<n/2)$ 个用户，那么从剩余的诚实用户中也能选出 $t+1$ 个用户完成门限签名，也就是说 TS 算法也能成功运行。

定理 2 在随机预言模型下，所提出的门限签名方案 NTS 能够抵抗利用选择消息进行存在性伪造攻击。

证明：在这里采用"模仿敌手观察"的方法[8, 9]实现证明，文[8]指出：若门限签名方案是可模仿的(Simulatable)，而对应的基础签名方案是安全的，则门限签名方案就是安全的(具有不可伪造性)，因此这里我们只需证明 NTS 方案是可模仿的即可。设 A 为 NTS 方案的 PPT 伪造敌手，它勾结了最多 t 个签名用户，并拥有发送方的组公钥 $Y=xP$、消息 m、m 的签名 $\sigma=(U,V)$ 和随机 Oracle H_1，H_2。

对于基于 GJKR 算法的密钥生成算法 TK 的可模仿性，文[6]已证明：对于敌手 A，存在一个模仿器(Simulator，一个 PPT 算法)SIM_1 模拟敌手 A 勾结的恶意用户和诚实用户联合执行 GJKR 算法(实际上是模仿 GJKR 算法)，得到的观察(view)，与实际执行 GJKR 算法得到的观察在敌手 A 看来是计算不可区分的。换一句话说，算法 TK 达到了保密性要求：任何少于 $t+1$ 个诚实的签名用户不能获得关于 x 的任何信息，其中 $t<n/2$。

下面证明 TS 算法的可模仿性。不失一般性，假设敌手 A 勾结的恶意用户为 $\Omega_B=\{P_1,P_2,\cdots,P_t\}$，诚实用户为 $\Omega_G=\{P_{t+1},P_{t+2},\cdots,P_n\}$。现在我们证明能够通过一个模仿器 SIM_2 来模仿敌手 A 执行 TS 算法以生成观察(view)和门限签名。对于恶意用户 Ω_B，其部分签名的生成及验证比较容易，关键是模仿诚实用户 Ω_G 的签名。由于 SIM_2 拥有 m 的签名 $\sigma=(U,V)$，则 SIM_2 可通过以下方法产生模仿敌手 A 执行 TS 算法的观察：

(1)若 $H_1(m,U)$ 和 $H_2(m)$ 未被询问过，则定义 $h=H_1(m,U)$，$Q=H_2(m)$。

(2)计算 $V_i=(r_i+hx_i)Q(1\leqslant i\leqslant t)$。设 $F(x)$ 为一个系数在 G_1^* 上的 t 次插值多项式，并满足 $F(0)=V$ 和 $F(i)=V_i$ $(1\leqslant i\leqslant t)$，计算 $V_i=F(i)(t+1\leqslant i\leqslant n)$ 并广播。

以上说明 TS 算法是可模仿的。换一句话说，对于一个拥有同样公钥 $Y=xP$ 的基础签名 QCXS 方案的伪造敌手 B，若 NTS 方案的敌手 A 能以一个不可忽略的概率伪造一个合法签名 σ，则敌手 B 就能以 σ 作为合法伪造，证毕。

结束语 门限签名实现了由一组签名用户共享对一个消息进行签名的功能，本质上是这组签名用户共享组私钥。由于 Boldyreva 门限签名方案不是概率型的签名体制，从而存在通过对比攻击而导致组私钥暴露的风险。本文基于 GDH 群构造了一个门限签名方案，并给出了安全性证明，该方案通过增加概率签名的特性，克服了 Boldyreva 方案的这一弱点。

参 考 文 献

1 Boneh D, Lynn B, Shacham H. Short Signatures from the Weil Pairing[A]. In: Proceedings of Asiacrypt'01, Lecture Notes in Computer Science 2248[C], Berlin: Springer-Verlag, 2001. 514～532

2 钱海峰，曹珍富，薛庆水. 基于双线性对的新型门限代理签名方案[J]. 中国科学，E 辑，2004，34(6)：711～720

3 Boldyreva A. Efficient Threshold Signature, Multisignature and Blind Signature Schemes Based on the Gap-Diffie-Hellman-Group Signature Scheme[A]. In: Proceedings of PKC 2003, Lecture Notes in Computer Science 2567[C], Berlin: Springer-Verlag, 2003. 31～46

4 Shamir A. How To Share A Secret[J]. Communications of the ACM, 1979, 22(11): 612～613

5 Pedersen T. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing[A]. In: Feigenbum, ed. Advances in Cryptology- Crypto'91, Lecture Notes in Computer Science 576[C], Berlin: Springer-Verlag, 1992. 129～140

6 Gennaro R, Jarecki S, Krawczyk H, et al. Secure Distributed Key Generation for Discrete-Log Based Cryptosystems[A]. In: Proceedings of the Eurocrypt'99, Lecture Notes in Computer Science 1592[C], Berlin: Springer-Verlag, 1999. 295～310

7 Feldman P. A Practical Scheme for Non-Interactive Verifiable Secret Sharing[A]. In: Proceedings of 28th IEEE Symposium on Foundations of Computer Science (FOCS' 87), 1987. 427～437

8 Gennaro R, Jarecki S, Krawczyk H, et al. Robust Threshold DSS Signatures[A]. In: Proceedings of the Eurocrypt'96. Lecture Notes in Computer Science 1070[C], Berlin: Springer-Verlag, 1996. 354～371

9 Micali S, Rogaway P. Secure Computation. In: Feigenbum, ed. Advances in Cryptology-Crypto'91, Lecture Notes in Computer Science 576. Berlin: Springer-Verlag, 1992. 392～404

10 陈伟东，冯登国. 签密方案在分布式协议中的应用[J]. 计算机学报，2005，28(9)：1421～1430

11 Baek J, Zheng Y L. Identity-Based Threshold Signature Scheme from the Bilinear Pairings[A]. In: Proceedings of International Conference on Information Technology: Coding and Computing (ITCC'04), Washington: IEEE Computer Society, 2004. 124～128