第 34 卷 第 5 期 计 算 机 工 程 2008 年 3 月
Vol.34 No.5 Computer Engineering March 2008
·安全技术· 文章编号：1000—3428(2008)05—0136—03 文献标识码：A 中图分类号：TP309

具有多个仲裁者的可验证加密签名方案及应用

彭长根[1,2]，樊玫玫[1,2]，李 祥[1]
(1. 贵州大学计算机软件与理论研究所，贵阳 550025；2. 贵州大学理学院数学系，贵阳 550025)

摘 要：可验证加密签名方案常用于构建公平交换协议，公平交换协议中的可信第三方往往会成为瓶颈。该文将 Boneh 等提出的单仲裁者可验证加密签名方案扩展为具有多个仲裁者的方案，方案应用无可信中心的可验证秘密共享技术实现了仲裁权力的分散。基于所构建的方案设计了一个公平合同签署协议，协议的可信第三方由多个仲裁者来构成，降低了第三方与其中一方合谋欺骗的风险。除此之外，协议具有不可伪造性、非透明性、公平性和机密性。由于该方案的设计是基于短签名方案和聚集签名方案，因此具有更高的通信效率。
关键词：可验证加密签名；聚集签名；仲裁者；合同签署协议

Verifiably Encrypted Signature Schemes and Its Applications with Multiple Adjudicators

PENG Chang-gen[1,2], FAN Mei-mei[1,2], LI Xiang[1]
(1. Institute of Computer Science, Guizhou University, Guiyang 550025;
2. Department of Mathematic, College of Sciences, Guizhou University, Guiyang 550025)

【Abstract】 Verifiably encrypted signature is usually applied to the fair exchange protocol. However the trusted third party (TTP) is a bottleneck in the fair exchange protocol with a TTP. This paper extends Boneh et al's verifiably encrypted signature with single adjudicator to a multi-adjudicator scheme. In this scheme, the adjudication can be shared among multiple adjudicators using verifiable secret sharing without trusted center. Based on the proposed verifiably encrypted signature scheme, it designs a contract signing protocol with multiple adjudicators. So the risk that any player colludes TTP can be reduced. In addition, the protocol can provide unforgeability, opacity, fairness and confidentiality. The scheme has lower communication cost due to short signature and aggregate signature.
【Key words】 verifiably encrypted signature; aggregate signature; adjudicator; contract signing protocol

交换协议的公平性在电商务活动中具有重要的意义。公平的交换协议除了交易的各方之外，一般还会涉及到可信的第三方(Trusted Third Party, TTP)，TTP在公平交换协议中充当仲裁者(adjudicator)的角色。但TTP往往会成为系统的瓶颈，特别是在完全可信模型中，因此，如何克服TTP的影响已成为一个主要研究问题。Boneh等在 2003 年基于他们自己的短签名方案[1]，提出了一个双线性聚集签名方案[2]，同时还基于该聚集签名方案构建了一个可验证加密签名方案(本文简称为BGLS_Vsig方案)。可验证加密签名方案在公平签约协议方面具有较好的应用[3-4]，文献[5]基于BGLS_Vsig方案设计了一个公平签名交换协议。在BGLS_Vsig方案中，只有一个仲裁者参与争议仲裁。为了防范仲裁者与其中一方合谋欺骗另一方的风险，本文建立一个具有多个仲裁者的可验证加密签名方案，以克服单个仲裁者权力过大的缺陷，利用无可信中心的可验证 (t,n) 门限秘密共享方案将仲裁权力分散给n个仲裁者共享，只有当n个中的t个或t个以上的仲裁者参与才能实现仲裁。随后基于所建立的方案，设计一个具有多个仲裁者(TTP)参与的公平签约协议，由于短签名具有签名长度短、计算简单的特点，因此本文方案在通信效率和计算效率方面具有较大的优势。

1 BGLS_Vsig方案[2]

设G_1，G_2，G_T为 3 个具有素数阶p的循环乘法群，其中 $p\geq 2^k$，k为安全参数；g_1和g_2分别为G_1 和G_2的生成元；$\psi: G_2 \to G_1$是一个可计算的同构映射，并有 $\psi(g_2)=g_1$；映射 $e: G_1 \times G_2 \to G_T$ 为一双线性对，群对 (G_1,G_2) 为co-GDH群[1]。BGLS_Vsig方案的安全性是基于从聚集签名中分解出个体签名的困难性假设，该方案描述如下：

(1)密钥生成算法：签名者随机选取私钥 $x\in_R Z_p$，公钥为 $v=g_2^x\in G_2$；同理得到仲裁者的私/公钥对为 $(x',v'=g_2^{x'})$。

(2)可验证加密签名生成算法：输入消息 $M\in\{0,1\}^*$ 和签名者私钥 x，首先计算 $h=H(M)\in G_1$，$\sigma=h^x$；然后随机选取 $r\in_R Z_p$，计算 $\mu=\psi(g_2)^r$ 和 $\sigma'=\psi(v')^r$；最后将 σ 和 σ' 聚集为 $\omega=\sigma\sigma'$。则 M 的可验证加密签名为 (ω,μ)。

(3)可验证加密签名的验证算法：输入 (v,v',M) 和 (ω,μ)，计算 $h=H(M)$，验证等式 $e(\omega,g_2)=e(h,v)e(\mu,v')$ 是否成立，若成立则签名有效。

(4)争议仲裁算法：输入 (v,x',v',M) 和 (ω,μ)，仲裁者验证 (ω,μ) 是否有效，若有效便输出 $\sigma=\omega/\mu^{x'}$。

2 具有多个仲裁者的可验证加密签名方案

BGLS_Vsig 方案只有一个仲裁者，为了限制仲裁者的权力，本节将 BGLS_Vsig 方案扩展为有多个仲裁者的可验证加密签名方案。

基金项目：贵州省自然科学基金资助项目(20052107)；贵州省省长基金资助项目(2005368)
作者简介：彭长根(1963－)，男，教授、博士，主研方向：密码学与信息安全；樊玫玫，硕士研究生；李 祥，教授、博士生导师
收稿日期：2007-03-10 **E-mail：**sci.cgpeng@gzu.edu.cn

2.1 方案描述

该方案涉及到的参数与 BGLS_Vsig 方案相同，方案由 5 个算法(*K, VESig, VESigVer, VESigAdj*)构成：

密钥生成算法 *K*：包括签名者的密钥生成算法 *KeyGen* 和仲裁者的密钥生成算法 *AdjKeyGen*。

KeyGen：签名者随机选取私钥 $x \in_R Z_p$，公钥为 $v = g_2^x \in G_2$。

AdjKeyGen：假设系统的*n*个仲裁者为 $\mathrm{T} = \{T_1, T_2, \cdots, T_n\}$，仲裁者的密钥分配算法采用Pederson[7]无需可信中心的可验证秘密共享(VSS)技术实现，每个仲裁者T_i都执行如下操作：

Step 1 随机选取 $x_i \in_R Z_p$ 作为私钥，计算 $c_i = g_2^{x_i} \in G_2$ 作为承诺广播给 T 中的其他成员T_j。

Step 2 随机选取 *t*-1 次多项式 $f_i(x) \in_R Z_p$：

$f_i(x) = f_{i,0} + f_{i,1}x + \cdots, f_{i,t-1}x^{t-1}$

这里有 $x_i = f_i(0) = f_{i,0}$；然后计算 $x_{ij} = f_i(j)$ (j＝1,2,⋯,n)和 $F_{ij} = g_2^{f_{i,j}}$ (j＝0,1,2,⋯,*t*-1)。

Step3 将 x_{ij} 通过安全信道传送给 $T_j (\forall j \neq i)$，并把 $\{F_{ij}\}_{i=1,2,\cdots,t-1}$ 广播给 T 中的其他成员T_j ($F_{i0} = c_i$ 之前已经广播)。

Step 4 通过式(1)验证从T_j 收到分享 x_{ji} 的正确性：

$$g_2^{x_{ji}} = \prod_{l=0}^{t-1} (F_{jl})^{i^l} \tag{1}$$

如果等式不成立，则拒绝T_j同时广播 x_{ji}，并停止协议。

Step5 如果所有T_j的分享 x_{ji} 都能通过Step 4 的验证，则计算 $x_i' = \sum_{j=1}^{n} x_{ji}$ 作为自己(即T_i)所持有组 *T* 的私钥 x' 的共享值(实际上组私钥为 $x' = \sum_{i=1}^{n} x_i'$)，同时计算 $v_i' = g_2^{x_i'}$ 并公开。

Step 6 计算 $v' = \prod_{i=1}^{n} c_i$ 作为组 T 的公钥并公开。

可验证加密签名生成算法 *VESig*：其算法与 BGLS_Vsig 的可验证加密签名生成算法相同，生成的加密签名为 (ω, μ)。

可验证加密签名的验证算法 *VEsigVer*：其算法与 BGLS_Vsig 的可验证加密签名验证算法相同。

争议仲裁算法 *VEsigAdj*：T 中的 *t* 个(或多于 *t* 个)仲裁者合作可以实现对可验证加密签名的解密，以对争议进行仲裁，假设这些成员集合记为 $A = \{T_i\}_{i \in \Phi}$，这里 $\Phi \subseteq \{1,2,\cdots,n\}$ 且 $|\Phi| = t$，*t* 为门限值。算法步骤如下：

Step 1 输入 (v, v'), $\{v_i'\}_{i=1,2,\cdots,n}$, *M* 和 (ω, μ)。

Step2 每个 $T_i \in A$ 可以用等式 $e(\omega, g_2) = e(h, v)e(\mu, v')$ 验证 (ω, μ) 的有效性，其中 $h = H(M)$。若 (ω, μ) 有效，输出解密份额 $\delta_i = \mu^{x_i'}$。

Step 3 对每个 $T_i \in A$ 输出的份额 δ_i，可以通过式(2)验证其有效性：

$$e(\delta_i, g_2) = e(\mu, v_i') \tag{2}$$

如果等式成立，则T_i提供的解密份额 δ_i 有效。

Step4 如果每个 $T_i \in A$ 提供的份额 δ_i 都有效，则计算 $\sigma = \omega / \prod_{i \in \Phi} \delta_i^{\pi_i}$，其中 $\pi_i = \prod_{j \in \Phi, j \neq i} \frac{-j}{i-j}$ 为 Lagrange 系数，σ 的有效性还可以通过式(3)进行验证：

$$e(\sigma, g_2) = e(h, v) \tag{3}$$

2.2 正确性分析

式(1)的正确性：

$$\prod_{l=0}^{t-1} (F_{jl})^{i^l} = \prod_{l=0}^{t-1} (g_2^{f_{i,j}})^{i^l} = g_2^{\sum_{l=0}^{t-1} f_{i,j} \cdot i^l} = g_2^{f_j(i)} = g_2^{x_{ji}}$$

式(2)的正确性：

$$e(\delta_i, g_2) = e(\mu^{x_i'}, g_2) = e(\mu, g_2^{x_i'}) = e(\mu, v_i')$$

门限解密过程的正确性：

$$\sigma = \omega / \prod_{i \in \Phi} \delta_i^{\pi_i} = \omega / \prod_{i \in \Phi} \mu^{x_i \pi_i} = \omega / \mu^{\sum_{i \in \Phi} x_i \pi_i} = \omega / \mu^{\sum_{i \in \Phi} f(i) \pi_i}$$

其中，$f(x) = \sum_{i=1}^{n} f_i(x)) = \omega / \mu^{x'}$ (由 Lagrange 公式得到)。

式(3)的正确性证明见文献[1]。

2.3 安全性分析

(1)具有不可伪造性(unforgeability)和非透明性(opacity)。在随机预言模型下，文献[2]证明了 BGLS_Vsig 方案具有在选择消息攻击下的不可伪造性和非透明性，本文方案是将 BGLS_Vsig 方案的单个仲裁者修改为多个仲裁者，但在加密签名时，仍用仲裁者的组公钥加密，因此对伪造者来说，其伪造能力和 BGLS_Vsig 方案一样，从而本文方案也具有不可伪造性；非透明性是指从可验证加密签名 ω 分解出原签名 σ 是困难的，该安全性是建立在聚集签名分离的困难性假设基础上的，从这个意义上来说，本文方案与 BGLS_Vsig 方案一样具有非透明性。

(2)实现了仲裁权力的分散。本文方案采用 (t,n) 秘密共享方案实现了由多个仲裁者共享仲裁权力，极大地降低了 TTP 的作用。仲裁者的密钥分配采用没有可信中心的可验证秘密共享方案进行，从而进一步提高了安全性。

(3)具有多种防欺骗的有效性验证。在 *AdjKeyGen* 算法阶段，利用式(1)可检验仲裁成员提供假密钥份额的欺骗；在 *VEsigAdj* 算法阶段，利用式(2)可验证仲裁成员提供假解密份额的欺骗；在共享解密完成后，还可以利用式(3)验证原签名 σ 的有效性。

3 一个具有公平性的合同签署方案

本节应用前一节提出的可验证加密签名方案，在文献[3,5]中方案的基础上，扩展设计一个由多个仲裁者构成 TTP 的公平合同签署方案。设 Alice 为合同发起人，Bob 为应答者，Alice 的私钥/公钥对为 $(x_A, v_A = g_2^{x_A})$，Bob 的私钥/公钥对为 $(x_B, v_B = g_2^{x_B})$；其他参数与第 2 节相同，其中，*M* 为要签署的合同文本。方案描述如下：

3.1 签名交换协议

Step 1 Alice 计算可验证加密签名 (ω_A, μ_A)：$h = H(M)$，$\sigma_A = h^{x_A}$，$r_A \in_R Z_p$，$\mu_A = \psi(g_2)^{r_A}$，$\sigma_A' = \psi(v')^{r_A}$，$\omega_A = \sigma_A \sigma_A'$；然后将 $\alpha = (M, \omega_A, \mu_A)$ 发送给 Bob。

Step 2 Bob 若能收到 Alice 的 α 并能验证通过，则计算可验证加密签名 (ω_B, μ_B)：$h = H(M)$，$\sigma_B = h^{x_B}$，$r_B \in_R Z_p$，$\mu_B = \psi(g_2)^{r_B}$，$\sigma_B' = \psi(v')^{r_B}$，$\omega_B = \sigma_B \sigma_B'$；然后将 $\beta = (M, \omega_B, \mu_B)$ 发送给 Alice；否则停止协议(quit)。

Step 3 Alice 若能收到 Bob 的 β 并能验证通过，则将签名 σ_A 发送给 Bob；否则执行 Abort 协议后退出。

Step 4 Bob 若能收到 Alice 的签名 σ_A 并能验证通过，则将签名 σ_B 发送给 Alice；否则执行 Resolve 协议后退出。

Step 5 Alice 若能收到 Bob 的签名 σ_B 并能验证通过，则正常退出，签名交换协议成功完成；否则，执行 Resolve 协议后退出。

3.2 仲裁协议

用于仲裁争议的协议有两个：Abort 协议和 Resolve 协议。

Abort协议：向每个仲裁者 $\{T_i\}_{i=1,2,\cdots,n}$ 发送中止协议的请求消息。每个T_i检查是否已执行过Resolve协议，若是则将

$(\omega_B, \mu_B^{x_i})$ 交给Alice；否则验证Alice的请求消息是否正确，若正确就发送一个允许中止协议标识AP_i给Alice和Bob。对于前一种情况，若Alice收到t个或t个以上的T_i的数据 $(\omega_B, \mu_B^{x_i})$，验证正确后就可以解密恢复出 σ_B；对于后一种情况，若Alice和Bob收到t个或t个以上的AP_i，Abort协议生效。

Resolve 协议：设 $X \in \{\text{Alice,Bob}\}$，$X$ 发送 $\{(\omega_A, \mu_A), (\omega_B, \mu_B)\}$ 给每个T_i。T_i首先检查Abort协议是否已执行，若已执行，则中止协议；否则验证X发送的数据是否正确，若正确则发送如下数据 γ_i 给X：

$$\gamma_i = \begin{cases} (\omega_B, \mu_B^{x_i}) & \text{当} X = \text{Alice} \\ (\omega_A, \mu_A^{x_i}) & \text{当} X = \text{Bob} \end{cases}$$

X 可通过等式(2)验证 γ_i 的有效性(将验证等式中的 δ_i 替换为 γ_i)。当 X 收到 t 个或 t 个以上的有效数据 γ_i，可以解密获得对方的签名。

3.3 协议分析

本协议除了具有不可伪造性和非透明性之外，还实现了公平性(fairness)：Alice和Bob双方要么都能获得对方的签名，要么都得不到。在签名交换协议中，利用两个子协议 Abort 和 Resolve 实现公平性。若 Alice 已发送 α 给 Bob，而收不到 Bob 的 β (因超时未收到，以下同)，则 Alice 可启动 Abort 协议中止交换；若 Bob 已发送 β 而收不到 σ_A，Bob 可以启动 Resolve 协议获得 σ_A；若 Alice 已发送 σ_A 给 Bob 而收不到 σ_B，Alice 可以启动 Resolve 协议获得 σ_B。

多仲裁者的方式实现了 TTP 权力的削弱，极大地约束了某一方与 TTP 合谋的欺诈行为。例如，Alice 已收到 β 而不发送 σ_A 给 Bob，却启动 Abort 协议进行欺骗，此时她需要勾结至少 t 个仲裁者才能从 β 解密出 σ_B。在仲裁协议的执行过程中，TTP 不参与对签名的解密，而是由每个仲裁者发送自己的解密份额给 Alice 或 Bob，由 Alice 或 Bob 来完成签名的解密，这更进一步保证了合同的机密性。并且在争议仲裁阶段，还能通过等式(2)验证各仲裁者提供假份额的欺骗。

本协议是优化(optimistic)的公平协议，即如果双方都严格按签名交换协议执行，争议不会发生，此时 TTP 不需要参与双方的交换，协议参与者只有 Alice 和 Bob。只有在争议出现时，TTP 才参与仲裁。在效率方面，由于 Boneh 的短签名方案和聚集签名方案具有签名短的优势，因而本文提出的协议与目前一些含多个可信第三方的公平交换协议相比，具有更高的通信效率和计算效率。

4 结束语

在公平交换协议中，TTP 往往会成为瓶颈，交易的一方与 TTP 合谋欺骗另一方的缺陷不易克服。因此，如何降低 TTP 在公平交换协议中的影响，成了当前普遍关注的研究问题，采用由多个仲裁者来构成 TTP 的方式不失为一种较好的途径。由于 Boneh 等人的可验证加密签名体制具有通信效率高和计算简便的优点，因此本文基于 Boneh 等人的方案所扩展的含有多个仲裁者的可验证加密签名方案，在构造含多个可信第三方的公平交换协议方面，更具有实用价值。另外，由于本文的方案是基于无可信中心参与的秘密共享技术，并且在争议仲裁阶段，仲裁成员不参与签名的合作解密，而仅发送自己的解密份额，这在敏感信息的签名交换场合有更好的适用性。

参考文献

[1] Boneh D, Lynn B, Shacham H. Short Signatures from the Weil Pairing[C]//Proceedings of Asiacrypt'01. Berlin: Springer-Verlag, 2001: 514-532.

[2] Boneh D, Gentry C, Lynn B, et al. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps[C]//Proceedings of Eurocrypt'03. Berlin: Springer-Verlag, 2003: 416-432.

[3] Asokan N, Shoup V, Waidner M. Optimistic Fair Exchange of Digital Signatures[J]. IEEE J. Selected Areas in Comm., 2000, 18(4): 593-610.

[4] Bao Feng, Robert H D, Mao Wenbo. Efficient and Practical Fair Exchange Protocols with Off-line TTP[C]//Proceedings of IEEE Symposium on Security and Privacy. Oakland: IEEE Press, 1998: 77-85.

[5] 李梦东, 杨义先, 马春光, 等. 利用双线性聚集签名实现公平的签名交换方案[J]. 通信学报, 2004, 25(12): 59-64.

[6] 张福泰. 具有分布式半可信第三方的公平交换协议[J]. 计算机工程, 2006, 32(3): 14-16.

[7] Pedersen T P. A Threshold Cryptosystem Without a Trusted Party[C]//Proc. of Eurocrypt'91. Berlin: Springer-Verlag, 1991: 522-526.

（上接第 135 页）

对登录请求包中的 host_name, host_name_ length, user_name, user_name_length 及 RPC 消息中的 name length, rpc name 都作了测试，名字字段保持不变，长度字段用负值、边界值填充。

登录请求时，由于其信息量比较大，因此往往被分成 2 个包，第 1 个包的 TDS 部分结构中包含多个相关字段：Host_name, Host_name_length, User_name, User_name_ length, Password, Password_length。在测试过程中，30 B 的 host_name 保持不变，host_name_length 只有 1 B，用负值 FF、边界 00 等特殊值填充。

4 结束语

本文利用基于块的协议分析方法编写了针对 TDS 协议的 Fuzzer 工具，利用这种基于 TDS 协议的安全分析测试技术可以帮助测试人员对某些感兴趣的部分进行集中测试，有效地发现 SQL Server 数据库可能存在的问题。目前只实现了数据转变、字符串、字段组合 3 种测试，随着对 TDS 协议的深入了解和各种新类型漏洞的出现，完善测试内容、提高测试覆盖率将是今后工作的重点。

参考文献

[1] Litchfield D, Grindlay B. SQL Server Security[M]. [S. l.]: McGraw-Hill Companies, 2004.

[2] Litchfield D, Anley C. The Database Hacker's Handbook[M]. [S. l.]: Wiley Publishing Inc., 2005.

[3] Aitel D. The Advantages of Block-based Protocol Analysis for Security Testing[Z]. Immunity Inc., 2002.

[4] Sprundel I. Fuzzing: Breaking Software in an Automated Fashion[D]. Holland: Eindhoven University, 2005.

[5] 雒 群, 刘秋实. 数据库通信协议分析与安全检测[DB/OL]. [2007-03-12]. http://www.edu.cn/20030826/3089816.shtml.