基于身份的强指定验证者签名的安全分析

秦志光，廖永建

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】针对基于身份的强指定验证者签名方案是不可授权的结论和基于身份的指定验证者代理签名方案设计，对两个方案进行安全性分析，首先证明了基于身份的指定验证者方案的签名是可授权的，然后证明了基于身份的指定验证者代理签名方案的签名是可伪造的，说明基于身份的强指定验证者签名方案的结论是不安全的；而基于身份的指定验证者代理签名方案的设计是不合理的。

关 键 词 攻击； 授权； 指定验证者签名； 代理签名

中图分类号 TP 309 **文献标识码** A doi:10.3969/j.issn.1001-0548.2009.05.033

Cryptanalysis of an ID-Based Designated Verifier Signature Schemes

QIN Zhi-guang and LIAO Yong-jian

(School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract Compared with ordinary digital signature, the designated verifier signature scheme makes it possible for a signer to convince a designated verifier that she has signed a message in such a way that the designated verifier cannot transfer the signature to a third party. In designated verifier signature scheme, no third party can even verify the validity of a designated verifier signature since it must use the designated verifier's secret key in verification. Recently, an ID-based strong designated verifier scheme, ID-based designated verifier proxy signature scheme, and partial cryptanalysis ware proposed. In this paper, we show that the designated verifier signature scheme is delegatable, and the designated verifier proxy signature is forgeable since construction of the proxy scheme is unreasonable.

Key words attack; delegatability; designated verifier signature; proxy signature

指定验证者签名是文献[1]引入的非交互式不可否认签名方案，它是指被指定的验证者能够验证签名是签名者的合法签名，然而它不可能使其他任何人相信这是签名者的合法签名，因为验证者自己也能产生合法的签名。也就是说，除了签名者和验证者，没有其他的人能产生合法的签名。

文献[1]还给出了一种增强的指定验证者签名的概念——强指定验证者签名。在强指定验证者签名方案中，仅仅被指定的验证者有能力验证签名。换句话说，在强指定验证者签名方案中，验证的过程中要使用被指定的验证者的私钥。文献[2]首先给出高效的强指定验证者签名方案的构造，文献[3-6]则提出了多种强指定验证者签名方案[3-6]。

文献[7]发现现有的各种指定验证者签名方案与文献[1]定义的指定验证者签名存在不一致，定义了一种新的、非标准攻击方法---——签名权的可授权攻击。它指签名者或验证者可把签名权委托给第3方(但不泄漏签名者和验证者的私钥)，而使第3方也能产生合法的签名。换句话说，除了签名者和验证者，还有被授权的第3方也能产生合法的签名，这是安全的(强)指定验证者签名方案不希望具有的性质。文献[9-10]证明了多个指定验证者签名方案是可授权的，并提出新的安全指定验证者签名方案。文献[11]证明另外几个指定验证者签名方案和强指定验证者签名方案[12-13]是可授权的，以及所有的基于双线性对的强指定验证者签名方案是可授权的。文献[14]针对存在强指定验证者签名方案虽然是(签名权)不可授权的、但验证是可授权的情况，提出了签名者身份的强保密性——在授权的条件下也保持签名者身份的保密性。

文献[6]提出的是新的基于身份的强指定验证者签名方案，并指出该方案是安全的，包括不可授权性。随后在此基础上提出了基于身份的指定验证者代理签名方案，但是未给出该方案的安全性分析。

收稿日期：2009－05－21
基金项目：国家自然科学基金(60803133)；博士点基金(200806140010)
作者简介：秦志光(1956－)，男，教授，博士生导师，主要从事信息安全方面的研究.

本文研究发现：文献[6]中基于身份的强指定验证者签名方案并不满足强指定验证者签名所有的性质，其签名权是可授权的；在代理签名中，虽然要求攻击者无法产生代理的授权，但是必须要能验证原始签名者对代理签名者存在授权，而基于身份的指定验证者代理签名方案由于设计的不合理，导致其是可伪造的。

1 基础知识

首先简要介绍本文将涉及的双线性对与相关的数学问题。

1.1 双线性对

假设G_1为素数q阶加法群，G_2为同阶乘法群，P为G_1的生成元，设$e:G_1\times G_1\to G_2$为具有下列性质的双线性映射。

(1) 双线性性：对所有的$P,Q\in G_1$，$a,b\in Z_q^*$等式$e(aP,bQ)=e(P,Q)^{ab}$成立；

(2) 非退化性：存在元素$P,Q\in G_1$满足$e(P,Q)\neq 1$，其中1为乘法群G_2的单位元；

(3) 可计算性：对所有的$P,Q\in G_1$，存在高效的算法计算$e(P,Q)$。

1.2 计算复杂性假设

由于在现有计算机理论研究中存在诸多用现有的图灵机理论尚无法高效解决的问题(如NP问题)。但计算机理论学家与密码学家们一直努力寻求高效地解决这些问题的方法。通常情况下，是假设上述问题为“难的”，即无高效解决方法的问题。对密码学家而言，更关心数论或代数曲线中如下具体的假设为“难的”一些问题。

(1) 离散对数问题(DLP)：已知$P,Q\in G_1$，如果存在整数$a\in Z_q^*$使得$Q=aP$，求a。

(2) 计算DH问题（CDHP）：对任何$a,b\in Z_q^*$，已知P、aP、bP，计算abP。

(3) 判定DH问题(DDHP)：对任何$a,b\in Z_q^*$，已知P、aP、bP、cP，判定等式$c=ab$是否成立。

(4) 双线性DH问题(BDHP)：随机选取$P\in G_1$和$aP,bP,cP\in G_1$，($a,b,c\in Z_q^*$未知)，计算$e(P,P)^{abc}$。

由于解决上述问题尚无高效的算法，因此假设上述问题为“难的”。下面给出BDHP假设的形式化定义。

BDH假设：如果Generator是BDH参数生成器，解决BDH问题的算法的优势$\mathrm{Adv}_{\mathrm{A}}(\cdot)$为算法A的输入$G_1$、$G_2$、$e$、$P$、$aP$、$bP$、$cP$，输出$e(P,P)^{\mathrm{abc}}$，其中$G_1$、$G_2$、$e$为Generator的输出，随机生成元$P\in G_1$，随机数$a,b,c\in Z_q^*$。BDH假设为对所有的高效的算法A，$\mathrm{Adv}_{\mathrm{A}}(\cdot)$是可忽略的。

2 基于身份的强指定验证者签名方案和基于身份的指定验证者代理签名方案

文献[6]在BDH假设的条件下，提出了基于身份的指定验证者签名方案，并在文献[15]的基础上，提出了基于身份的指定验证者代理签名方案。

2.1 基于身份的指定验证者签名方案

(1) 系统参数建立(setup)：私钥生成中心(PKG)选取阶为q的素数阶GDH(gap diffie-hellman)加法群G_1和同阶的乘法群G_2，双线性映射$e:G_1\times G_1\to G_2$和生成元$P\in G_1$。PKG选取随机数$s\in Z_q^*$，并计算$P_{\mathrm{pub}}=sP$得到相应的公钥。选取两个密码Hash函数$H_1:\{0,1\}^*\to G_1$和$H_2:\{0,1\}^*\times G_1\times G_1\to G_1$。最后设主密钥为$s$，系统参数为$(G_1,G_2,P,P_{\mathrm{pub}},H_1,H_2,e,q)$。

(2) 密钥提取算法(key extract)：已知用户的身份ID，PKG计算$S_{\mathrm{ID}}=sH_1(\mathrm{ID})$，作为其私钥通过安全信道发送给身份为ID的用户。

(3) 签名算法：签名者Alice生成消息M的指定验证者(Cindy)签名σ，选取随机数$r\in Z_q^*$，且计算$U=rQ_{\mathrm{IDA}}$、$V=H_2(M,e(rQ_{\mathrm{IDC}},S_{\mathrm{IDA}}))$和签名$\sigma=(U,V)$。

(4) 验证算法：被指定的验证者Cindy收到签名σ后，接受签名，当且仅当$V=H_2(M,e(U,S_{\mathrm{IDC}}))$等式成立。

(5) 模拟算法：被指定的验证者选择随机数$r'\in Z_q^*$，且计算$U'=r'Q_{\mathrm{IDA}}$和$\sigma=H_2(M,e(U',S_{\mathrm{IDS}}))$。

文献[6]对该方案进行了安全分析，指出该方案是正确的、强的、不可否认的，同时可以证明它是不可授权的。

2.2 基于身份的指定验证者代理签名方案

在该方案中，除了密码Hash函数H_2外，系统参数与密钥提取算法与上述方案中的算法相同。其中$H_2:\{0,1\}^*\times G_2\to G_1$。

1) 代理密钥生成算法：原始签名者Alice生成消息M的指定验证者(Cindy）签名σ,选取随机数$r\in Z_q^*$，且计算$U=rQ_{\mathrm{IDA}}$和$V=H_2(W,e(rQ_{\mathrm{IDB}},S_{\mathrm{IDA}}))$，其中$W$是记录了原始签名者与代理签名者等信息的委任书，$Q_{\mathrm{IDB}}$是代理签名者Bob的公钥，Alice把$(U,W,V)$发送给Bob，Bob接受

签名，当且仅当等式$V=H_2(M,e(U,S_{\mathrm{IDB}}))$成立。

2) 代理签名算法：Bob计算消息M的代理签名，Bob选取随机数$t\in Z_q^*$，且计算$X=tQ_{\mathrm{IDB}}$、$S_{\mathrm{IDP}}=t^{-1}V+S_{\mathrm{IDB}}$和$Y=H_2(M,W,e(tQ_{\mathrm{IDC}},S_{\mathrm{IDP}}))$，Bob把$(M,W,V,X,Y)$发送给被指定的验证者Cindy。

3) 代理签名验证算法：被指定的验证者Cindy收到签名(M,W,V,X,Y)后，验证如下过程。

(1) 检查消息M是否符合委托书W委托的范围，如果不是，则停止，反之则继续；

(2) 检查Alice和Bob是否分别是委托书W中的原始签名者和代理签名者；

(3) 如果上面过程通过，Cindy接受签名当且仅当等式$Y=H_2(M,W,e(Q_{\mathrm{IDC}},V)\ e(S_{\mathrm{IDC}},X))$成立。

3 两个方案的安全性分析

3.1 指定验证者签名方案的授权攻击

可授权性是指在指定验证者签名方案中存在可产生签名的知识，但无法从该知识中提取出签名者或被指定的验证者的私钥。

文献[6]指出强指定验证者签名方案是不可授权的，但是没有给出严格的证明。本文拟证明该方案的签名权是可授权的，即证明对任何第3方D，在得到$e(Q_{\mathrm{IDC}},S_{\mathrm{IDA}})$的情况下，是无法得到签名者和验证者的私钥的；同时只要其知道$e(Q_{\mathrm{IDC}},S_{\mathrm{IDA}})$，就能产生合法的签名。

D选取随机数$r\in Z_q^*$，且计算$U=rQ_{\mathrm{IDA}}$和$V=H_2(M,e(Q_{\mathrm{IDC}},S_{\mathrm{IDA}})^r)$，得到签名$\sigma=(U,V)$。很容易验证签名$\sigma$能使等式$V=H_2(M,e(U,S_{\mathrm{IDC}}))$成立。而且$e(Q_{\mathrm{IDC}},S_{\mathrm{IDA}})$是签名者与被指定的验证者都能产生的知识(被指定的验证者计算$e(S_{\mathrm{IDC}},Q_{\mathrm{IDA}})$。

在得到$e(Q_{\mathrm{IDC}},S_{\mathrm{IDA}})$或$e(S_{\mathrm{IDC}},Q_{\mathrm{IDA}})$的条件下，由双线性函数$e$的性质可知是无法计算出签名者的私钥$S_{\mathrm{IDA}}$和被指定的验证者的私钥$S_{\mathrm{IDC}}$。

所以该方案符合文献[7]定义的可授权性。至此，所有的基于双线性对的强指定验证者签名方案都是可授权的。

3.2 基于身份的指定验证者代理签名是可伪造的

首先，在代理密钥生成的过程中使用了强指定验证者，因此任何除签名者(原始签名者)与被指定的验证者(代理签名者)外第3方都无法验证(U,W,V)的合法性，所以此过程可以是公开信道，也可以是秘密信道。一方面使想验证签名的合法性的用户(可能产生代理密钥的攻击者)无法验证签名，另一方面又使需要验证代理授权的用户(被指定的验证者Cindy)也无法验证签名合法性。因此也为伪造消息M的签名提供可能，其过程如下。

(1) 委托书伪造：伪造者产生委托书W，其中包括原始签名者Alice和代理签名者Bob，以及消息M是否符合委托书W委托的范围。

(2) 签名伪造：伪造者选取随机数$r\in Z_q^*$和$V\in G$，计算：

$$X=rP$$

$$Y=H_2(M,W,e(Q_{\mathrm{IDC}},V)e(Q_{\mathrm{IDC}},rP_{\mathrm{pub}}))。$$

设消息M的签名为(M,W,V,X,Y)，由于在验证算法中，没有验证者对代理签名者的授权的验证，伪造者可以根据其自身目的产生委托书W，其内容包括原始签名者Alice和代理签名者Bob，以及消息M是否符合委托书W委托的范围等诸多信息。

(3) 验证签名。由产生W的过程，很明显伪造的签名能过程验证算法的前两个条件，又因为：

$$H_2(M,W,e(Q_{\mathrm{IDC}},V)e(S_{\mathrm{IDC}},X))=$$
$$H_2(M,W,e(Q_{\mathrm{IDC}},V)e(QS_{\mathrm{IDC}},sX))=$$
$$H_2(M,W,e(Q_{\mathrm{IDC}},V)e(Q_{\mathrm{IDC}},srP))=$$
$$H_2(M,W,e(Q_{\mathrm{IDC}},V)e(Q_{\mathrm{IDC}},rP_{\mathrm{pub}}))=$$
$$H_2(M,W,e(Q_{\mathrm{IDC}},V)e(Q_{\mathrm{IDC}},rP_{\mathrm{pub}}))=Y$$

所以，如果被指定的验证者Cindy接受该签名，即伪造成功。

4 结 论

本文证明基于身份的强指定验证者签名方案是可授权的；而基于身份的指定验证者代理签名方案由于设计不合理，导致其是可伪造的。

参 考 文 献

[1] JAKOBSSON M, SAKO K, IMPAGLIAZZO R. Designated verifier proofs and their applications[C]//Advances in Cryptology-EuroCrypt. Berlin: Springer Heidelberg, 1996: 143-154.

[2] SAEEDNIA S, KREMER S, MARKOWITCH O. An efficient strong designated verifier signature scheme[C]//The international conference on information security and cryptology. Seoul: Springer Berlin\Heidelberg, 2003: 40-54.

[3] LAGUILLAUMIE F, VERGNAUD D. Designated verifier signatures: anonymity and efficient construction from any bilinear map[C]//The Sixth Conference on Security and Cryptography for Networks. Amalfi: Springer, Berlin/Heidelberg 2004: 105-119.

[4] HUANG X, SUSILO W, MU Y, et al. Short(identity-based) strong designated verifier signature schemes[C]//The Information Security Practice and Experience Conference. Hangzhou: Springer Berlin/Heidelberg, 2006: 214-225.

[5] SUSILO W, ZHANG F, MU Y. Identity-based strong

designated verifier signature schemes[C]//The Conference on Information Security and Privacy. Sydney: Springer Berlin / Heidelberg 2004, 313-324.
[6] KANG B，BOYD C, DAWSON E. Identity-based strong designated verifier signature schemes: attacks and new construction[J]. Computers and Electrical Engineering, 2009, 35: 49-53.
[7] LIPMAA H, WANG G, BAO F. Designated verifier signature schemes: attacks, new security notions and a new construction[C]//International Colloquium on Automata, Languages and Programming. Lisboa: Springer Berlin/Heidelberg, 2005: 459-471.
[8] SAEEDNIA S, KREMER S, MARKOWITCH O. An efficient strong designated verifier signature scheme[C]//The International Conference on Information Security and Cryptology. Seuol: Springer, Berlin/Heidelberg, 2003: 40-54.
[9] LAGUILLAUMIE F , VERGNAUD D. Designated verifier signatures: anonymity and efficient construction from any bilinear map[C]//The Conference on Security and Cryptography for Networks. Amalfi: Springer Berlin/膜 Heidelberg, 2004: 105-119.
[10] STEINFELD R, WANG H, PIEPRZYK J. Efficient extension of standard schnorr/RSA signatures into universal designated-verifier signatures[C]//Public Key Cryptography. Singapore: Springer Berlin/Heidelberg, 2004: 86-100.
[11] LI Y, LIPMAA H, PEI D. On delegatability of four designated verifier signatures[C]//The International Conference on Information and Communications Security. Beijing: Springer Berlin/Heidelberg, 2005: 61-71.
[12] SUSILO W, ZHANG F, MU Y. Identity-based Strong Designated Verifier Signature Schemes[C]//The Conference on Information Security and Privacy. Sydney: Springer Berlin/Heidelberg, 2004: 313-324.
[13] LAGUILLAUMIE F, VERGNAUD D. Multi-designated Verifiers Signatures[C]//The 6th International Conference on Information and Communications Security. Malaga: Springer Berlin/Heidelberg, 2004, 495-507.
[14] 廖永建, SUSILO W, 陈抗生. 强指定验证者签名的不可授权性[J]. 浙江大学学报(工学版), 2009, 43(2): 334-337.
LIAO Yong-jian, SUSILO W, CHEN Kang-sheng. On non-delegatability property of strong designated verifier signature[J]. Journal of Zhejiang University (Engineering Science), 2009, 43(2): 334-337.
[15] LAL S, VERMA V. Identity base strong designated verifier proxy signature schemes[DB/OL]. [2009-05-16]. http://eprint. iacr.org/complete/2006/394.pdf.

编 辑 熊思亮

秦志光，教授，1996年在电子科技大学获工学博士学位，现为电子科技大学计算机学院教授、博士生导师、国家特殊津贴获得者、四川省学术和技术带头人，主要从事信息安全方面的研究。担任中国计算机学会理事，教育部高等学校信息安全类教学指导委员会委员，教育部高等学校实验室建设指导委员会委员，国家自然科学基金同行评议专家，国家科技部、教育部同行评议专家，国家信息安全成果产业化基地(西部)专家组成员，四川省计算机用户协会理事长，四川省软件行业协会常务副理事长，四川省计算机学会副理事长，四川省科技厅电子信息技术专家组成员，四川省保密技术专家咨询小组成员，四川省软件企业认定专家组成员，国家软件评测中心认证专家，四川省咨询业协会教授级咨询师，国际电子电器工程师学会(IEEE)会员，多份核心期刊编委。近年来，先后在各种重要期刊或国际学术会议上发表学术论文80余篇(其中SCI、EI检索10余篇)，获得四川省、重庆市科技进步二等奖各一项、四川省科技进步三等奖一项、国防科学技术三等奖一项、成都市科技进步二等奖和三等奖各一项；获得软件著作权登记6项、专利3项。主持国家自然科学基金、国家863计划、国家计算机网络与信息安全管理中心、博士点基金、军事预研、四川省科技攻关等研究项目多个。