ELGamal 类签名中的阈下信道封闭问题研究

董庆宽 牛志华 肖国镇
(西安电子科技大学综合业务网国家重点实验室 西安 710071)

摘 要 设计了一个新的阈下信道封闭协议,完全封闭了 ELGamal 类签名中存在于随机会话密钥中的阈下信道.在该协议中看守 W 虽然参与了协议的执行,但不能伪造签名,从而保证了签名者的签名权力.同时该文的方案也可以看作是一种新的带审批权的签名方案,必须由看守和签名者合作才能打开签名.最后给出 DSA 中的阈下信道完全封闭协议.

关键词 数字签名;阈下信道封闭协议;阈下信道;信息隐藏
中图法分类号 TP309

Research on the Freeness of Subliminal Channels in ElGamal-Type Signatures

DONG Qing-Kuan NIU Zhi-Hua XIAO Guo-Zhen
(*National Key Laboratory of Integrated Services Networks*, *Xidian University*, *Xi'an* 710071)

Abstract A new subliminal-free protocol in ElGamal-Type signatures is designed. Our design is a three-turn interactive protocol between the warden and the signer in which the warden covers all the data generated by the signer and finishes the signature, but he can not forge the signatures. It is the first time that subliminal channels exiting in random session keys in ElGamal-Type signatures are completely avoided. Our design can be viewed as a signature scheme with the warden's examining and approving. The signer must cooperate with the warden to open the signature. Finally, a subliminal-free protocol in DSA is given.

Keywords digital signature; subliminal-free protocol; subliminal channel; information hiding

1 引 言

阈下信道,也称潜信道,最早是由 Simmons 于 1983 年提出的在签名或认证协议中建立起来的一种隐蔽信道[1].Simmons 通过一个在看守(warden)的完全监视下,两个囚犯如何协商一个逃跑计划的例子引入了该信道,并且作了大量的研究.1993 年,Simmons 在 DSA 的随机会话密钥中引入了四个阈下信道[2](我们假设消息 m 的 DSA 签名为(r,s),其中 $r=g^k \bmod p \bmod q$,详见第 2 节),其中的宽带信道是通过在收发双方之间共享签名秘密钥来实现的;另外三个窄带的信道包括:(1)通过控制签名成份 r 对某秘密模数的二次剩余特性,使之与阈下比特相适应来构造信道;(2)通过搜索适合的 r 使之最后 u 比特($u\geq 1$)等于待传的 u 比特阈下消息所构造的信道;(3)根据具有较短指数的离散对数的可解性构造的信道.这些信道同样存在于 ElGamal 签名中.不久 Simmons 又提出了封闭该信道的一个协议[3],之后 Desment 等对此作了深入的研究,并于 1996 年在文献[4]中建立了一个失败终止式阈下信道,从而指出了文献[3]中的 Simmons 的协议并不能完全

收稿日期:2003-06-23;修改稿收到日期:2004-03-10.本课题得到国家自然科学基金重大项目(90104005)、国家"九七三"重点基础研究发展规划项目基金(G1999035804,2003F06)资助.**董庆宽**,男,1973 年生,博士研究生,主要研究方向为密码学、网络安全及信息伪装技术.E-mail:dqkromantic@sina.com.**牛志华**,女,1976 年生,博士研究生,主要研究方向为信息安全与密码学.**肖国镇**,男,1934 年生,教授,博士生导师,主要研究方向为密码学、编码学和信息论.

封闭阈下信道.针对此 Simmons 于 1998 年在文献[5]中进行了详细分析,并采用分割选择的方式进行封闭,使容量尽可能的小,但仍不能实现完全封闭,而且封闭所达到的容量越小,计算复杂度和通信量上所付出的代价越大.自 1998 年至今,人们对封闭问题的研究进展比较缓慢,没有更好的结果,因此如何设计一个能够对阈下信道完全封闭的协议是值得研究的一个课题.

本文设计了一个新的阈下信道的封闭协议,完全封闭了 ELGamal 类签名中存在于随机会话密钥中的阈下信道.在该协议中看守 W 虽然参与了协议的执行,但不能伪造签名,从而保证了签名者的签名权力.同时我们的方案也可以看作是一种新的带审批权的签名方案,必须由看守和签名者合作才能打开签名.最后给出 DSA 中的阈下信道完全封闭协议.论文的第 2 节简单回顾了 ELGamal 签名和 DSA,在第 3 节具体给出了我们所设计的交互式封闭协议,第 4 节对该协议进行了详细的分析,第 5 节给出了 DSA 中的实现,文章最后给出小结.

2 ELGamal 签名和 DSA

2.1 ELGamal 签名[6]

用户密钥的产生如下:p 是一个大素数,$g\in F_p^*$ 是一个生成元;签名秘密钥 $x\in\{1,2,\cdots,p-2\}$,相应的公开密钥 $y=g^x \bmod p$.对消息 m 的签名:签名者(signer)首先计算 $H(m)$,H 为标准的哈希(Hash)函数,并把 $H(m)$简记为 H(以下同),满足$0\leq H<p-1$,随机选择 $k\in_R\{1,2,\cdots,p-2\}$且 $gcd(k,p-1)=1$.签名者计算 $1\leq r<p$,$r=g^k \bmod p$,$s=k^{-1}(H-xr) \bmod (p-1)$,$(s,r)$即为有效的签名.接收者通过检验 $1\leq r<p$ 及 $g^H=(r^s y^r) \bmod p$,来验证签名的正确性.

2.2 DSA[7]

用户的公钥选取如下:大素数 $p\geq 512$ 比特,q 为 160 比特的素数且满足 $q\mid p-1$,$g\in Z_p$ 是一个阶为 q 的元素,$y=g^x \bmod p$,其中 x 是均匀随机选取的签名秘密钥($0<x<q$).一个对消息 m 的签名如下:签名者(signer)首先计算哈希值 H,然后选取随机数 k,$0<k<q$,计算 $r\equiv(g^k \bmod p) \bmod q$,以及 $s\equiv k^{-1}(H+xr) \bmod q$.二元组$(r,s)$即为该消息的签名.消息的验证通过如下等式 $r=(g^{(Hs^{-1}) \bmod q} y^{(rs^{-1}) \bmod q} \bmod p) \bmod q$.

3 封闭协议的设计

不论是 1993 年 Simmons 的封闭协议还是后来 1998 年提出的分割选择法的封闭协议,之所以不能达到完全封闭的目的,是因为阈下发方即签名者可以控制或选择签名算法的输出,而这些输出能被收方得到,在传输过程中看守不再对此进行修改,也就是说签名的最终完成者是阈下发方.针对此,在下面提出的新设计方案中,我们令看守 W 参与签名的生成,并且使 W 没有伪造签名的能力,从而在保证签名者的签名权力的前提下,实现对信道的完全封闭.产生 ELGamal 签名的一个新的交互式协议如下:

SET-UP 阶段,看守 W 随机选择整数 t($0<t<p-1$,$gcd(t,p-1)=1$),计算 $T=g^t \bmod p$,保密 t,公开 T.秘密的选取两个大整数 e,d 满足 $ed\equiv 1 \bmod (p-1)$.签名者 A 发布其签名公钥为 $Y=T^x \bmod p$.

协议执行如下:

1.W 秘密选取随机数 k',满足 $0<k'<p-1$ 及 $gcd(k',p-1)=1$,计算 $\alpha=g^{k'e} \bmod (p-1)$,发送 α 给签名者 A;

2.A 秘密选取随机数 k,满足 $0<k<p-1$ 及 $gcd(k,p-1)=1$,计算 $\beta=\alpha^k \bmod p$,发送 β 给 W;

3.W 计算 $r=\beta^d=g^{k'ked}=g^{k'k} \bmod p$,$u=r/\beta \bmod (p-1)$,$\theta=u^{-1}t^{-1} \bmod (p-1)$,发送 θ 给 A;

4.A 计算 $s=k^{-1}(H\theta-x\beta) \bmod (p-1)$发送$(m,s)$给 W;

5.W 计算 $s'=sk'^{-1}\theta^{-1}=k'^{-1}k^{-1}(H-xtu\beta) \bmod (p-1)$,其中 $u\beta=r \bmod (p-1)$,产生签名(r,s')发送给接收者 R.R 验证签名的正确性为 $g^H=r^{s'}Y^r \bmod p$.

4 分 析

4.1 签名的安全性

令 $k''=k'k$,$X=xt$,最终接收者拿到的签名(r,s')可简单的表示为 $r=g^{k''} \bmod p$,$s'=k''^{-1}(H-Xr)\cdot \bmod (p-1)$,这与普通的 ElGamal 签名没什么分别.已经证明对除看守之外的任何第三方是安全的.

下面我们来看一下看守是否有伪造签名的可能.看守选取的秘密参数主要有 t,k',但不知道 x,k,在步 5 之前看守不知道被签消息 H 以及 H,x,k 之间的关系,无从伪造,因而伪造的唯一机会是在步 5,此时看守 W 得到如下方程

$$s=k^{-1}(H\theta-x\beta) \bmod (p-1) \qquad (1)$$

则他要伪造 A 的签名,有下面三种情况可以考虑:

情况 1. 如果他要伪造的消息的哈希值 H'满足 $H'=j^{-1}H$,即 $H=jH'$,则将其带入式(1)可得

$s=k^{-1}(H'j\theta-x\beta)\bmod(p-1)$. 两边再乘以 $j^{-1}\theta^{-1}$ 得到 $s''=sj^{-1}\theta^{-1}=k^{-1}(H'-xj^{-1}\theta^{-1}\beta)=k^{-1}(H'-xtj^{-1}u\beta)\bmod(p-1)$,为产生有效的签名,$W$ 必须求解关于 z 的方程 $j^{-1}u\beta=j^{-1}r=g^{zk'k}\bmod p$,即 $j^{-1}r=r^z\bmod p$,然后他计算 $s'=s''z^{-1}k'^{-1}\bmod(p-1)$ 和 $r'=g^{zk'k}\bmod p$ 从而完成签名. 显然如果 j,z 均不可逆那么伪造不成立,如果可逆那么求解 z 相当于求解离散对数 $z=\log_r(j^{-1}r\bmod p)$,这是困难的,因此伪造不成立.

情况 2. W 可以考虑在步 3 选择值 j_0 并计算 $\theta=u^{-1}t^{-1}j_0^{-1}$ 发给 A,在步 5 以 $j_0^{-1}\theta^{-1}k'^{-1}=utk'^{-1}$ 乘以方程(1)得到 $s''=k'^{-1}k^{-1}(Hj_0^{-1}-xtu\beta)\bmod(p-1)$,然后寻找消息 m',使其哈希值满足 $H'=j_0^{-1}H$,这相当于寻找 Hash 函数的一个碰撞,而这对于所采用的安全的哈希函数来说是困难的. 因此不能伪造.

情况 3. 在步 5,W 可以首先计算 $G=r^{k'^{-1}}=g^k\bmod p$,选择值 $a,0<a<p-1$,计算 $r'=rG^{-a}=g^{(k'-a)k}\bmod p$,然后以 $\theta^{-1}G^a(k'-a)^{-1}$ 乘以方程(1)的两边可得 $s''=(k'-a)^{-1}k^{-1}(HG^a-xtr')\bmod(p-1)$,然后寻找消息 m' 使其哈希值 H' 满足 $H'=G^aH$,如情况 2 所述这相当于寻找安全哈希函数的一个碰撞,是困难问题. 反之先选取 H',求出 $j=H'/H\bmod(p-1)$(假设 H 的模 $p-1$ 的逆存在),以 j 乘以式(1)两边,再求关于 a 的方程 $G^a=j\bmod p$ 以计算值 $k'-a$ 来产生有效签名,而这相当于求解离散对数,是困难问题,因而不能伪造.

由此可见 W 不能伪造签名. 当然 W 既然允许无害消息传递,那么它也必须完成协议,进而完成正确的签名.

4.2　完全封闭性

除了验证公钥 Y, 接收者唯一能够获得的是签名 (r,s'),签名者要传递阈下消息必须以二者为载体. 由于直至 W 完成最终签名之前 A 都对 k',$g^{k'}$ 一无所知,因而也就不能控制 (r,s') 的值. 由协议可以看出,尽管 A 能够得到 $\alpha(=g^{k'e}\bmod(p-1))$ 和 $\theta(=u^{-1}t^{-1}\bmod(p-1))$,但由于他不知道秘密指数 e,d 及秘密参数 t,u,所以不能获得关于 k',$g^{k'}$ 的任何信息. A 仅能获得 $T^\theta=g^{u^{-1}}$ 而该值对收方来说是不可见的.

显然,不知道 k',$g^{k'}$ 也就无法计算签名 (r,s'),其中 $r=(g^{k'})^k\bmod p$,$s'=s\theta^{-1}k'^{-1}\bmod(p-1)$. 可见发送者不能传递任何阈下消息给接受者. 因此该协议实现了对随机会话密钥所引入的阈下信道的完全封闭.

4.3　关于签名权力

这个协议可以看作是一个带审批权的签名体制,签名者签署的消息必须经过看守的审批盖章方能生效. 需要注意的是要打开签名必须由看守和 A 合作来进行. A 是主签名人决定要传递的无害消息,看守是审批人,对消息进行审批和转发,但不能伪造签名. 看守可以通过公开 t 来释放审批权限.

4.4　复杂度及通信量

Simmons 于 1996 年设计的协议(简称 SIM96,见文献[3])中,在看守和签名者之间共需两次数据交互,而且协议执行期间共需计算两次模指数运算,通信量和复杂度相当小,这里只考虑模指数复杂度,因为与模指数运算相比较,模乘和模加等运算的复杂度可以忽略. 而为了减小可能引入的阈下信道的容量,他于 1998 年设计的协议(简称 SIM98, 见文献[5])尽管也是两次交互,但由于引入了分割选择技术,每次至少要传输 n 组数据(n 为分割选择样本数)这使通信量增长 n 倍. 而且每次通信至少要计算 n 个模指数,复杂度非常高.

本文所设计的协议中共需 3 次数据交互和 3 次模指数计算,较之 SIM96 仅各增加了 1 次,通信量和复杂度略有增加,而相对于 SIM98 来说却是一种极大的简化,我们以很小的代价实现了对会话密钥的完全封闭.

5　DSA 中的封闭协议

DSA 与 ELGamal 签名的差别在于签名作用的子群不同,只要把以上在 $p-1$ 子群上的运算改成在 q 阶子群上的运算就可以了,DSA 算法如 2.2 节所述,我们的协议如下:

SET-UP 阶段,看守 W 随机选择整数 $t,0<t<q$,计算 $T=g^t\bmod p$,保密 t, 公开 T. 秘密的选取两个大整数 e,d 满足 $ed\equiv1\bmod q$. 签名者 A 发布其签名公钥为 $Y=T^x\bmod p$. 其中 g 为 q 阶产生元,$q\mid p-1$.

协议执行如下:

1. W 秘密选取随机数 k',满足 $0<k'<q$,计算 $\alpha=g^{k'e}\bmod p$,发送 α 给签名者 A;

2. A 秘密选取随机数 k,满足 $0<k<q$,计算 $\beta=\alpha^k\bmod p$,发送 β 给 W;

3. W 计算 $\eta=\beta^d=g^{k'ked}=g^{k'k}\bmod p$,$r=\eta\bmod q$,$u=r/\beta\bmod q$,$\theta=u^{-1}t^{-1}\bmod q$,发送 θ 给 A;

4. A 计算 $s=k^{-1}(H\theta+x\beta)\bmod q$ 发送 (m,s) 给 W;

5. W 计算 $s'=sk'^{-1}\theta^{-1}=k'^{-1}k^{-1}(H-xtu\beta)\bmod q$,其中 $u\beta=r\bmod q$,产生签名 (r,s') 发送给接收者 R.

R 验证签名的正确性为

$$r = (g^{(Hs'^{-1})\bmod q} Y^{(rs'^{-1})\bmod q} \bmod p) \bmod q.$$

具体分析同第 3 节,不再赘述.

6 结 论

本文设计了一种新的阈下信道封闭协议,首次解决了 ELGamal 类签名中由随机会话密钥所引入的阈下信道的完全封闭,严格说是计算上完全封闭的,依赖于离散对数求解的困难性和哈希函数的安全性.对于其他类型体制中的阈下信道是否能用该协议,有待于进一步的研究.

参 考 文 献

1 Simmons G. J.. The prisoner's problem and the subliminal channel. In: Proceedings of the CRYPTO'83, New York, 1984, 51～67

2 Simmons G. J.. The subliminal channel in the U. S. Digital Signature Algorithm(DSA). In: Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography-SPRC'93, Rome, Italy, 1993, 35～54

3 Simmons G. J.. An introduction to the mathematics of trust in security protocols. In: Proceedings of Computer Security Foundations Workshop VI. Franconia, New Hampshire: IEEE Computer Society Press, 1993, 121～127

4 Desmedt Y.. Simmons' protocol is not free of subliminal channels. In: Proceedings of the 9th IEEE Computer Security Foundations Workshop, County Kerry, Ireland, 1996, 170～175

5 Simmons G. J.. Results concerning the bandwidth of subliminal channels. IEEE Journal on Selected Areas In Communications, 1998,16(4): 463～473

6 ElGamal T.. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 1985, 31(4): 469～472

7 Digital Signature Standard(DSS). A Proposed Federal Information Processing Standard (FIPS) Publication 186, 1994

DONG Qing-Kuan, born in 1973, Ph. D. candidate. His research interests include cryptography, network security and information hiding.

NIU Zhi-Hua, born in 1976, Ph. D. candidate. Her main research interests include cryptography and information security.

XIAO Guo-Zhen, born in 1934, professor, Ph. D. supervisor. His research interests include cryptography, coding and information theory.

Background

The subject, "Research on the fundamental problems and models of information collection and analysis in network", is mainly supported by National Outstanding Nature Science Foundation.

The motivation of the subject is to present the theory and their realizable algorithms of the detection and judgment of data integrity and the characteristics of signals by acquiring and analyzing the information dynamically and fast transmitted in network. Further, the purpose of the subject is to present a systemic cryptanalysis theory and models, to obtain a new feasible analyzing method on information security and a realized system, to promote the research on the solution of open difficult mathematical problems and theoretical cryptography and to discover new theories and methods. In this work the modern mathematical theory and the new type subject in the cross-fields between the computer science and mathematics are applied and Source coding, error-correct coding and cryptanalysis are synthetically considered. The researches include: (1) Capturing, analyzing and processing the mega-information in network and some new methods about that; (2) the design, analysis and realization of the feasible integral solution of information security; (3) New theoretical cryptography; (4) Information hiding and steganography; (5) Other relative applying problem, such as cryptostandards.

We have made some progress in provable secure public-key cryptosystems, secure protocols, information hidings, and so on. This paper is to deal with the problems of completely avoiding subliminal channels in signatures, part of the information hiding. This paper is also partially supported by 97-3 Project and Shaanxi Nature Science Foundation.