Schnorr 签名方案的一种攻击*)

刘景美　王新梅
(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　Schnorr 签名算法计算量少，速度快，在灵巧卡中具有大量的应用，因此必须具有足够的安全性。本文给出了选择消息下对 Schnorr 签名方案的一种攻击方法，攻击者可以假冒签名者进行签名；另外给出了一种攻击签名者私钥的选择消息攻击方法，其攻击性不依赖于离散对数的求解问题。

关键词　Schnorr，签名，安全性分析

Cryptanalysis of Schnorr Signature Scheme

LIU Jing-Mei　WANG Xin-Mei
(National Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071)

Abstract　Schnorr signature is widely used in smart card with little computation and high rate, so it should be enough secure. In this paper a method is presented to forge the signature of Schnorr signature scheme, and we also present a key-recovery attack against the Schnorr signature algorithm under the chosen messages. All the attack actions do not depend on the computation of discrete logarithm.

Keywords　Schnorr, Signature, Cryptanalysis

1　引言

数字签字在信息安全，包括身份认证、数据完整性、不可否认性以及匿名性等方面都有重要应用，特别是在大型网络安全通信中的密钥分配、认证以及电子商务系统中具有重要作用，它是实现电子贸易、电子支票、电子货币、电子购物、电子出版及知识产权保护等系统安全的重要保证。目前大多数的数字签字都是基于大整数分解或离散对数计算的困难性等数学难题，如 1978 年出现的基于大整数分解困难性的 RSA[1] 签字体制和 1985 年出现的基于离散对数计算困难性的 ElGamal[2~7] 签字体制和 ElGamal 签字体制变形后的 Schnorr[8] 签字体制。已被定为美国数字签字标准 DSS 的签字算法 DSA 就是在 ElGamal 和 Schnorr 签字体制的基础上设计的。Schnorr 签名算法计算量少，速度快，在灵巧卡中具有大量的应用，因此必须具有足够的安全性。本文继续对 ElGamal 签字体制的变形 Schnorr 签字体制进行了分析，发现 Schnorr 签字体制在选择消息的情况下是不安全的，不仅可以假冒签名者进行签名，而且可以求出签名者的私钥，攻击性不依赖于离散对数的求解问题。

2　Schnorr 签名方案

1989 年 C. Schnorr 提出的基于离散对数的数字签名方案是一种随机化的签名机制，其签名方案是：

1. 体制参数

p，q：大素数，q|p−1，q 是大于等于 160bit 的整数，p 是大于 512bit 的整数，保证 Z_p 中求解离散对数为困难问题；

g：Z_p^* 中元素，且 $g^q \equiv 1 \bmod P$，也就是说 g 是 Z_p^* 中子群 Z_p^* 的一个生成元；

μ：消息空间，为 Z_p^*；

ζ：签字空间，为 $Z_p^* \times Z_p$；

x：用户秘密钥 $x \in Z_q^*$；

$y \equiv g^x \bmod p$

密钥：$\kappa=(p,g,a,y)$，其中 p,g,y 为公钥，x 为秘密钥。

2. 签字过程

1)选择秘密随机数 $\kappa \in Z_q$；

2)计算 $r=g^k \bmod p$

$s=k+xH(r \| M) \bmod (p-1)=k+xe \bmod (p-1)$，式中 $e=H(r \| M)$；

3)将 $Sig_k(M,k)=S=(r,s)$ 作为签字，将 $M,(r \| s)$ 送给对方，其中 $r \| s$ 表示 r 与 s 的数字串的级连。

3. 验证过程

收信人收到消息 M 及签字 $(r \| s)$ 后，(1)计算 $e=H(r \| M)$；(2)计算 $r'=g^s y^{-e} \bmod p$；(3)验证 $Ver_k(M,r,s) \Leftrightarrow H(r' \| M) \equiv e \bmod p$，若等式成立，则 (r,s) 是对消息 M 的签字，理

*)基金项目：国家 973 项目(G1999035804)；“十五”国家密码发展基金。刘景美　博士研究生，研究方向：网络安全和密码分析学。

参 考 文 献

1　Wu T. The secure remote password protocol. In: Proceedings of the Internet Society Network and Distributed System Security Symposium, 1998. 97～111

2　Wu T. The SRP Authentication and Key Exchange System. Stanford University, September 2000. Request For Comments (RFC)2945

3　Wu T. SRP-6: Improvements and Refinements to the Secure Remote Password Protocol. 2002

4　OASIS. Web Service Security: SOAP Message Security 1. 0. OASIS Standard 200401, 2004

由如下：

因为若$(r \| s)$是M的合法签字，则：

$r'=g^s \square y^{-e} \equiv g^{k+xr} g^{-xr} \equiv g^k \equiv r \bmod p$

因此可以保证 $H(r' \| M) \equiv H(r \| M) \equiv e \bmod p$

在此方案中，对同一消息 M，由于随机数 k 不同而有不同的签字值 $S=(r \| s)$。

3 对 Schnorr 签名方案的伪造攻击

Schnorr 签名方案在防止第三者的伪造签名方面存在不安全的因素，下面的研究结果表明攻击者可以选择一个符合要求的合法签名来伪造他人签名，使得验证者将伪造的签名当作是合法的签名，并且不能发现签名的伪造性。鉴于 Schnorr 签名方案攻击的困难性在于计算离散对数[9~17]，我们另辟新径，从而避开离散对数的计算以保证攻击的准确性和容易性。

方法一 伪造(r,s)的攻击

攻击者收集签名者的正确签名集 M_1，$(r_1 \| s_1)$和 M_2，$(r_2 \| s_2)$，若需要签名的消息为 M'，然后进行如下计算：

(1)计算 $r'=r_1 \cdot r_2 \bmod p \Rightarrow r'=g^{k_1} \square g^{k_2} \bmod p$

(2)计算 $e'=H(r' \| M') \bmod p$

(3)计算 $e_1=H(r_1 \| M_1) \bmod p$

(4)计算 $e_2=H(r_2 \| M_2) \bmod p$

若集合中有签名使得 $e' \equiv e_1+e_2 \bmod p$，则攻击者可以选择这个签名集 M_1，$(r_1 \| s_1)$和 M_2，$(r_2 \| s_2)$来实施攻击行为，然后进行后续的计算：$s'=s_1+s_2 \bmod p \Rightarrow s'=k_1+xe_1+k_2+xe_2=k_1+k_2+x(e_1+e_2) \bmod p$

则 M'，$(r' \| s')$就是攻击者假冒签名者进行的正确签名。证明过程如下：

$g^{s'} y^{-e'} = g^{s_1+s_2} g^{-xe'} = g^{k_1+k_2+x(e_1+e_2)} g^{-x(e_1+e_2)} = g^{k_1+k_2} = r' \bmod p$

验证成功，因此假冒者伪造签名成功，也就是说只要攻击者选取一个满足要求的合法签名，则攻击者可以伪造任何人进行合法的签名，因此说 Schnorr 签名方案是及其不安全的。签于一般签名的特殊性质，即任何人都可以验证签名的有效性，签名者可以对多份文件进行签署，只要攻击者选取了任何一个需求的签名，就可以伪装签名者进行非法的签名。已发现的对 Schnorr 签名方案的伪造签名大多都存在离散对数的求解问题，实际中能否进行有效的攻击还难以确定，本攻击方案的提出无疑给签名的安全性提出了新的挑战。

方法二 对私钥 a 的攻击

另外，攻击者可以不用像上述过程来进行伪造签名，而是直接攻击签名者的私钥，攻击过程也是选取签名集合，验证签名是否满足如下的关系：

$y^t \equiv 1 \bmod p \Rightarrow g^{xt} \equiv 1 \bmod p$

若对某一签名满足上式，则就选择这个签名进行攻击，因为 g 是 Z_p^* 中子群 Z_q^* 的一个生成元，即

$g^q \equiv 1 \bmod p$

所以 $g^{xt}=g^{tq}$

即 $xe=tq$

于是 $x=tqe^{-1} \bmod p$

其中 t 的计算过程为：

$t=0$;

while($y^t \neq 0$){

$y^t=y^t/g^{p-1}$;

$t++$;}

从而求出了签名者的私钥，攻击者可以利用签名者的私钥来对任意的消息进行签名。下面来看一下这种攻击的概率分析。

攻击的重点是 $y^t=g^{xt} \equiv 1 \bmod p$，因为 $g^q \equiv 1 \bmod p$，所以 $q \mid xe$，也就是说 $\gcd(x,q) \neq 0$ 或 $\gcd(e,q) \neq 0$。因为 a 是一个未知量，我们就从已知量 e 出发来分析。设$\{\beta\}=\{\gamma : \gamma \mid q\}$，不同的 γ 对应不同的 e 值，则 e 出现的概率为 $p(r)=1/q-1-\Phi(q)$，其中 $\Phi(q)$表示 q 的欧拉函数值，也就是 Z_q 中与 q 互素的元素的个数，只要指定不同的 e_i，则就可以求出具体的私钥 x_i 的个数 $\| \beta_i \|$，$i=1,2,\cdots, \| \beta \|$。因此满足式子 $q \mid xe$ 的 xe 出现的概率为 $p(xe)=\sum_{i=1}^{\beta} \| \beta_i \| /[q-1-\Phi(q)]$，若 $\Phi(q)$很大，则 $q \mid xe$ 将以很大的概率出现，也就是说攻击者选择不多的正确签名就可以攻击成功。

结论 Schnorr 签名方案在防止第三者的伪造签名方面存在不安全的因素，攻击者可以任意选择一个合法的签名来伪造他人的合法的签名，使得验证者将伪造的签名当作是合法的，并且不能发现签名的伪造性。已发现的对 Schnorr 签名方案的伪造签名大多都存在离散对数的求解问题，实际中能否进行有效的攻击还难以确定。本文提出的非基于离散对数的攻击方案无疑给签名的安全性提出了新的挑战。

参 考 文 献

1 Rivest R L, Shamir A, Adleman L M. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 1978, 21(2): 120～126

2 ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms. Advances in Cryptology-CRYPTO' 84 Proceedings, Springer-Verlag, 1985. 10～18

3 Tsiounis Y, Yung M. On the Security of ElGamal Based Encryption. Springer-Verlag, 1998, 1431: 117

4 Jakobsson M, Juels A. Addition of ElGamal Plaintexts. Springer-Verlag, 2000, 1976: 346

5 Bleichenbacher D. Generating ElGamal Signatures without Knowing the Secret Key. Springer-Verlag, 1996, 1070: 10

6 Shparlinski I E. On the Uniformity of Distribution of the ElGamal Signature. Springer-Verlag, 13(1): 9～16

7 Ferreira L C, Dahab R. Optimistic Blinded-Key Signatures for ElGamal and Related Schemes. Springer-Verlag, 2004, 3824: 254

8 Schnorr C P. Efficient signature generation for smart cards. Advances in cryptology-crypto' 89 proceedings, Springer-Verlag, 1991. 239～252

9 Schnorr C P. Security of Blind Discrete Log Signatures against Interactive Attacks. Springer-Verlag, 2001, 2229: 1

10 Hühnlein D. Faster Generation of NICE-Schnorr-Type Signatures. Springer-Verlag, 2001, 2020: 1

11 Nguyen P Q, Shparlinski I E. The Insecurity of the Digital Signature Algorithm with Partially Known Nonces. Journal of Cryptology, 15(3): 151～176

12 Mahassni E E, Nguyen P Q, Shparlinski I E. The Insecurity of Nyberg-Rueppel and Other DSA-Like Signature Schemes with Partially Known Nonces. Springer-Verlag, 2001, 2146: 97

13 Naccache D, M'Raïhi D, Vaudenay S, et al. Can D. S. A. Be Improved?: Complexity Trade-offs with the Digital Signature Standard. Springer-Verlag, 1995, 950: 77

14 Giraud C, Knudsen E W. Fault Attacks on Signature Schemes. Springer-Verlag, 2004, 3108: 478～491

15 Naccache D, Nguyên P Q, Tunstall M, et al. Experimenting with Faults, Lattices and the DSA. Springer-Verlag, 2005, 3386: 16

16 Blake I F, Garefalakis T. On the Security of the Digital Signature Algorithm, Springer-Verlag, 26(1-3): 87～96

17 Howgrave-Graham N A, Smart N P. Lattice Attacks on Digital Signature Schemes. Springer-Verlag, 23(3): 283～290