改进的 Rabin 密码体制安全性分析

李子臣[1], 王永传[2], 曾志峰[2], 杨义先[2], 吴伟陵[2]
(1. 焦作工学院计算机科学与技术系, 焦作 454159; 2. 北京邮电大学信息安全中心, 北京 100876)

摘 要: Shamir 和 Schorr 对 Rabin 数字签名方案提出一种有效的攻击方法, 称为 Shamir 攻击. 为了避免 Shamir 攻击, 本文提出一种有效的比特位扰乱法(Bit Perturbation) . 基于 Rabin 公钥密码体制, Harn 和 Kiesler 提出一种改进的公钥密码体制、数字签名方案和认证加密方案. 本文指出 Harn 和 Kiesler 提出的密码体制是不安全的, 并设计一种安全的数字签名方案.

关键词: 数字签名; 密码体制; 二次剩余
中图分类号: TN918.14 文献标识码: A 文章编号: 0372-2112 (2000) 03-0128-03

Cryptanalysis of Improved Rabin's Cryptosystem

LI Zi-chen[1], WANG Yong-chuan[2], ZENG Zhi-feng[2], YANG Yi-xian[2], WU Wei-ling[2]
(1. Depart. of Computer Science and Technology, Jiaozuo Institute of Technology, Jiaozuo 454159, China;
2. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: Shamir and Schorr proposed an attack to Rabin's digital signature. The attack is called Shamir attack. In this paper, we will present a new and efficient bit perturbing method to avoid the Shamir attack. Harn and Kiesler proposed a public-key cryptosystem, digital signature and authentic encryption scheme based on Rabin's cryptosystem. In this paper, we will point out these cryptosystem are insecure and we also propose a secure digital signature scheme.

Key words: signature; cryptosystem; quadratic residues

1 引言

Rabin 根据 RSA 密码体制提出一种数字签名方案[1]. 这种方案的安全性建立在素因子分解之上, 伪造有效的签名等价于一个大数的素因子分解. 文献[2]中, Shamir 和 Schnorr 对 Rabin 方案提出一种攻击方法, 称为 Shamir 攻击. 为了避免 Shamir 攻击, 本文提出一种新的比特位扰乱法(Bit Perturbation). 在文献[3]中, Harn 和 Kiesler 对 Rabin 方案进行了改进, 提出一种改进的公钥密码体制、数字签名方案和认证加密方案. 本文对这些密码体制的安全性进行分析, 提出两种新的攻击方法, 指出这些密码体制在新的攻击方法下是不安全的, 并提出一种安全的数字签名方案.

2 Shamir 攻击

在本文中, p, q 是两个大素数, p= 3mod 4, q= 3 mod 4, n = pq, J(a/ n) 表示 Jacobi 符号, QR_n 表示[1, n- 1]中所有二次剩余, QNR_n 表示[1, n- 1]中所有二次非剩余.

在 Rabin 方案中, 公钥: (n, b) , 其中 n, b 为 500 比特的数, bI [1, n- 1]. 私钥: (p, q) . 如果签名 s 和消息 m 满足方程: m= s(s+ b) mod n, 称 s 为消息 m 的有效签名. 上述 Rabin 签名方案的安全性等价于大数 n 的素因子分解[4]. 就是如果攻击者能够对模数 n 素因子分解, 那么攻击者可以获得用户的私钥(p, q) , 对任意的消息 m 可以伪造有效的签名.

Shamir 和 Schnorr 根据 Morrison-Brillhart 素因子分解算法(称为 M-B 素因子分解算法)[5, 6], 对 Rabin 数字签名方案提出一种攻击方法. 假定在 Rabin 方案中, 对消息签名之前要对 m 的低 k 比特位进行扰乱. 攻声明者说服签名者对消息 $m= b^2/4 \bmod n$ 进行多次签名或者从已知的消息和签名组中可以获得多个同余方程:

$$d_i = (sc_j)^2 \bmod n,\ i = 1, 2, \quad (1)$$

其中: $|d_i| = k$, $|d_i|$ 为 d_i 的比特位数. 利用 M-B 素因子分解算法可以对大数 n 进行素因子分解, 其复杂度为:

$$O(f(|n|))\, e^{c\sqrt{\ln k}}$$

其中: f 为一多项式. 当 $k < |n|/2$ 时, 利用上述算法很容易的将大数 n 进行素因子分解, 从而获得用户的私钥. 在 Rabin 数字签名方案中, k= 60, |n| = 500, 攻击者利用 M-B 素因子分解算法对公钥 n 进行素因子分解, 从而可以对任意的消息伪造有效的签名, 因此 Shamir 攻击是一种有效的攻击方法.

3 有效的避免 Shamir 攻击的新方法

由 Shamir 攻击方法可见, 根据 Rabin 方案中消息的比特位扰乱法, 可以产生多个特殊同余方程, 利用 M-B 素因子分

收稿日期: 1998-12-04; 修订日期: 1999-02-23
基金项目: 国家自然科学基金(No. 69772035, 69882002, 69896240) 资助课题

解算法对公钥 n 进行素因子分解. 为了避免 Shamir 攻击, 下面设计一种具有新的比特位扰乱法的数字签名方案.

选择 k n | n|, 且| d| = | b| = k.

公钥: (n, b) , H 为一公开函数, 其定义如下:

$$H(m)=\begin{cases} m-m_k+d, & \text{若}|m|\ E\ |n|-k \\ d@2^{|n|-k}+m+d, & \text{若}|m|<|n-k| \end{cases}$$

其中, m_k 是消息 m 的低 k 比特位所产生的数.

私钥: (p, q).

签名过程: 对消息 m, 签名者计算 H(m) , 从方程 H(m) = s(s+ b) mod n 解出 s, 则 s 为消息 m 的签名.

验证过程: 验证者收到消息签名组(m, s) 后, 计算 H(m) , 验证方程 H(m) = s(s+ b) mod n 方程是否成立. 如果等式成立签名有效, 否则签名无效.

在上述签名方案中, Shamir 攻击是无效的.

事实上: 由 Shamir 攻击方法, 令 m= - b^2/ 4 mod n, 说服签名者对消息 m 进行签名. 假定 s 为消息 m 的签名, 满足方程: H(m) = s(s+ b) mod n.

因为 k n | n|, | m| < | n| - k, 所以 H(m) = d @$2^{|n|-k}$+ m+ d mod n.

令 s= sc- b/ 2 mod n, H(m) = $(sc)^2$- b^2/ 4 mod n,

$$d@2^{|n|-k}+d=(sc)^2 \bmod n$$

当 n 充分大, k 充分小时, | d @$2^{|n|-k}$+ d| 接近于| n| .

利用 M- B 素因子分解算法可以对数 n 进行素因子分解, 其复杂度为:

$$O(f(|n|)\,e^{c\sqrt{\ln n \ln\ln n}})$$

因此 Shamir 攻击无效.

4　对 H2K 认证加密方案的两种攻击方法

Harn 和 Kiesler 提出一种明文和密文 1 比 1 的 Rabin 公钥密码体制、数字签名和认证加密方案, 分别称为 H2K 公钥密码体制、H2K 数字签名方案和 H2K 认证加密方案. 下面对 H2K 认证加密方案提出两种新的攻击方法.

411　H2K 认证加密方案

假设系统中有两个用户 A, B. 在通信之前用户要分别产生公钥和私钥.

密钥产生过程: 用户 i 公钥: (n_i, A_i, B_i, C_i) , 私钥: (p_i, q_i) . 其中: i I {A, B}, n_i= p_iq_i, A_i I QR_{p_i} H QNR_{q_i}, B_i I QNR_{p_i} H QR_{q_i}, C_i I QNR_{p_i} H QNR_{q_i}.

在产生公钥和私钥时要求 n_A> n_B, 由文献[7, 8] 知, 这一条件很容易实现.

加密过程: 用户 A 利用用户 B 的公钥对消息 m 进行加密 C= m^2 V_B mod n_B,

其中 $V_B=\begin{cases} 1, & J(m/n_B)=1,\ 0<m<n_B/2 \\ A_B, & J(m/n_B)=1,\ n_B/2<m<n_B \\ B_B, & J(m/n_B)=-1,\ 0<m<n_B/2 \\ C_B, & J(m/n_B)=-1,\ n_B/2<m<n_B \end{cases}$

签名过程: 用户 A 用私钥对 C 进行签名, Cc= P(C) , 其中 P 为比特位扰乱函数, 计算 S= $(CcV_A)^{1/2}$ mod n_A, 其中

$$V_A=\begin{cases} 1, & Cc\ I\ QR_{P_A}\ H\ QR_{q_A} \\ A_A, & Cc\ I\ QR_{P_A}\ H\ QNR_{q_A} \\ B_A, & Cc\ I\ QR_{P_A}\ H\ QR_{q_A} \\ C_A, & Cc\ I\ QNR_{P_A}\ H\ QNR_{q_A} \end{cases}$$

S 分别满足

$$\begin{matrix} J(S/n_A)=1, & 0<S<n_A/2 \\ J(S/n_A)=1, & n_A/2<S<n_A \\ J(S/n_A)=-1, & 0<S<n_A/2 \\ J(S/n_A)=-1, & n_A/2<S<n_A \end{matrix}$$

S 为用户 A 对消息 m 的签名, 将签名组(C, S) 通过公用信道传输给用户 B.

签名过程: 用户 B 收到(C, S) , 利用 A 的公钥对签名进行验证, 首先计算 Cc= P(C) , 验证方程: S^2= CcV_A mod n_A, 其中

$$V_A=\begin{cases} 1, & J(S/n_A)=1,\ 0<S<n_A/2 \\ A_A, & J(S/n_A)=1,\ n_A/2<S<n_A \\ B_A, & J(S/n_A)=-1,\ 0<S<n_A/2 \\ C_A, & J(S/n_A)=-1,\ n_A/2<S<n_A \end{cases}$$

. 如果方程成立, 签名有效, 否则签名无效.

解密过程: 用户 B 利用私钥对 C 可以解密,

计算 m= $(CV_B^{-1})^{1/2}$ mod n_B, 其中

$$V_B=\begin{cases} 1, & CI\ QR_{P_B}\ H\ QR_{q_B} \\ A_B, & CI\ QR_{P_B}\ H\ QNR_{q_B} \\ B_B, & CI\ QR_{P_B}\ H\ QR_{q_B} \\ C_B, & CI\ QNR_{P_B}\ H\ QNR_{q_B} \end{cases}$$

且 m 分别满足

$$\begin{matrix} J(m/n_B)=1, & 0<m<n_B/2 \\ J(m/n_B)=1, & n_B/2<m<n_B \\ J(m/n_B)=-1, & 0<m<n_B/2 \\ J(m/n_B)=-1, & n_B/2<m<n_B \end{matrix}$$

, 那么 m 就是用户 A 发送到用户 B 的消息

下面对 H2K 认证加密方案提出两种攻击方法

412　基于签名的攻击方法

对于一攻击者, 从 A 和 B 的通信中可以获得许多签名(C_i, S_i) , i= 1, 2, , , 且满足 S_i^2= CcV_A mod n_A, 其中 Cc_i= P(C) ,

$$V_A=\begin{cases} 1, & J(S_i/n_A)=1,\ 0<S_i<n_A/2 \\ A_A, & J(S_i/n_A)=1,\ n_A/2<S_i<n_A \\ B_A, & J(S_i/n_A)=-1,\ 0<S_i<n_A/2 \\ C_A, & J(S_i/n_A)=-1,\ n_A/2<S_i<n_A \end{cases}$$

.

从集合(C_i, S_i) , i= 1, 2, , 中选择 C_i^*, 满足条件| (C_i^*) c V_A^*| F k, 并令 d_i^*= (C_i^*) c* V_A^*, 则有一组方程:

$$(S_i^*)^2=d_i^* \bmod n_A.$$

如果选择 k< (1/ 2) | n| , 利用 M2B 素因子分解方法可以很容易对 n_A 进行素因子分解. 那么攻击者可以获得用户 B 的私钥, 因此 H2K 认证加密方案是不安全的.

413　已知明文的攻击方法

假定攻击者从用户 A 和 B 的通信中, 获得多组明文以及

对应的密文(m_i, C_i), $i=1,2,\ldots$. 由用户 A 的加密过程可以得到: $C_i = m_i^2 V_B \bmod n_B$, 其中

$$V_B=\begin{cases}1, & J(m_i/n_B)=1, \quad 0<m_i<n_B/2\\ A_B, & J(m_i/n_B)=1, \quad n_B/2<m_i<n_B\\ B_B, & J(m_i/n_B)=-1, \quad 0<m_i<n_B/2\\ C_B, & J(m_i/n_B)=-1, \quad n_B/2<m_i<n_B\end{cases}$$

即 $C_i V_B^{-1} = m_i^2 \bmod n_B$.

从(m_i, C_i)中选择 C_i^* 使得 $|C_i^* (V_B^*)^{-1}| F k$, 令 $d_i^* = C_i^* (V_B^*)^{-1}$, 有 $d_i^* = (m_i^*)^2$.

如果选择 $k<(1/2)|n_B|$, 利用 M2B 素因子分解方法可以很容易对 n_B 进行素因子分解. 因此攻击者在可以获得用户 B 的私钥, 所以在已知明文的攻击下 H2K 认证加密方案是不安全的.

在文献[3]中, Harn 和 Kiesler 同时还提出了 H2K 公钥加密体制和 H2K 数字签名方案. 对于 H2K 数字签名方案, 利用本文提出的第一种攻击方法同样可以对模数 n 进行素因子分解, 因此 H2K 数字签名也是不安全的. 对于 H2K 公钥加密体制利用本文提出的第二种攻击方法, 在已知明文的休条件下, 同样可以对模数 n 进行素因子分解, 因此 H2K 公钥加密体制在已知明文攻击下, 也是不安全的.

5 新 H2K 数字签名方案

511 新的 H2K 数字签名方案

为了产生新的数字签名方案, 选择 $k<|n|$, $|d|=k$, 构造函数:

$$H(m)=\begin{cases}m-m_k+d, & 若|m|E|n|-k\\ d@2^{|n|-k}+m, & 若|m|<|n|-k'\end{cases}$$

其中, m_k 是消息 m 的低 k 比特位所产生的数.

下面构造新的 H2K 数字签名方案.

公钥: (n, A, B, C), 私钥: (p, q), 其中 $n=pq$, $A\in QR_p \cap QNR_q$, $B\in QNR_p \cap QR_q$, $C\in QNR_p \cap QNR_q$.

签名过程: 对消息 m, 计算 $S=(H(mV))^{1/2} \bmod n$, 其中:

$$V=\begin{cases}1, & m\in QR_p \cap QR_q\\ A, & m\in QR_p \cap QNR_q\\ B, & m\in QR_p \cap QR_q\\ C, & m\in QNR_p \cap QNR_q\end{cases}$$

且 S 分别满足

$$\begin{cases}J(S/n)=1, & 0<S<n/2\\ J(S/n)=1, & n/2<S<n\\ J(S/n)=-1, & 0<S<n/2\\ J(S/n)=-1, & n/2<S<n\end{cases}$$

那么 S 为消息 m 的签名.

验证过程: 验证者接收到(m, S)后, 计算 $mV \bmod n$, 其中:

$$V=\begin{cases}1, & J(S/n)=1, \quad (0<S<n/2)\\ A, & J(S/n)=1, \quad (n/2<S<n)\\ B, & J(S/n)=-1, \quad (0<S<n/2)\\ C, & J(S/n)=-1, \quad (n/2<S<n)\end{cases}$$

计算 $H(mV) \bmod n$, 验证 $S^2 = H(mV) \bmod n$, 若等式成立, 签名有效, 否则签名无效.

512 新的 H2K 数字签名方案安全性分析

在新的 H2K 数字签名方案中, 签名验证方程为: $S^2 = H(mV) \bmod n$, $H(mV) \cap QR_n$. 由文献[4]可得到, 从上述方程直接计算消息 m 的签名 S 相当于大数 n 的素因子分解. 另外在函数 H(m)的构造中, 当 n 很大时, $|H(m)|$接近于$|n|$. 因此 Shamir 攻击和本文提出的两种攻击方法对于上述新的 H2K 数字签名方案是无效的.

6 结论

本文对 Rabin 数字签名方案提出了一种新比特位扰乱方法, 由这种新的比特位扰乱方法所构成的数字签名方案能够避免 Shamir 攻击. 对 H2K 密码体制提出两种新的攻击方法, 在这两种攻击方法下, H2K 公钥密码体制, 数字签名, 认证加密方案都是不安全的. 对于 H2K 数字签名方案提出了一种新的 H2K 数字签名方案, 这种新的方案能够对抗 Shamir 和本文提出的攻击方法, 但对于 H2K 公钥密码体制和 H2K 认证加密方案需要进一步的研究.

参考文献

[1] M. Rabin. Digital signatures and public key functions as intractable as factorization. MIT Tech. Report. LCS/TR2212, 1979

[2] A. Sahmir and C. P. Schorr. Cryptanalysis of certain variants of Rabincs signature scheme. Inf. Process. Lett., Oct, 1984: 113~115

[3] L. Harn and T. Kiseler. Improved Rabin. s scheme with high efficiency. Electron. Lett., 25 may 1989, 25(11): 716~728

[4] 卢开澄. 计算机密码学. 清华大学出版社, 1998

[5] M. Morrison and J. Brillnart. A method of factorization and the factoi2ization of F7, Mathematics of Computation 1975, 29: 183~205

[6] D. E. Kunth. The art of computer programming. Vol. 2 (Addison2Wes2ley, Reading, MA, 2, 1981)

[7] R. L. Rivest, A. Shamir and L. Adelman. A method for obtaining digital signatures and public2key cryptosystem. Commun. ACM, Feb. 1978, 21: 120~126

[8] L. M. Kohnfelder. On the signature reblocking problems. In complexity of computer computations (Plenum Press, NY, 1978): 85~104

李子臣 1964 年出生, 1995 年获北京理工大学硕士学位, 1999 年获北京邮电大学信息工程系博士学位. 主要研究领域: 现代密码学, 计算机网络安全. 已有多篇文章发表.