文章编号:1674-7070(2009)03-0223-06

基于消息恢复型 Rabin-PSS 的无线局域网认证方案

刘佳[1,2]　韦宝典[1,3]　戴宪华[1]

摘要

基于无线局域网非对称的结构特点,设计了一个基于公钥密码技术的身份认证方案,并在成功认证的同时实现会话密钥的分配. 该方案充分利用 Rabin-PSS-MR 签名方案和 ElGamal 改进型签名方案中签名与验证计算量的非对称性,合理地配置认证服务器 AS 与移动终端 STA 的操作,使网络的整体响应效率得以极大的提高;同时,Rabin-PSS-MR 签名方案的消息恢复功能减少了公钥证书认证过程的传输量(仅传输公钥证书而不传输公钥),大大节省了通信带宽.

关键词

无线局域网;认证;Rabin-PSS-MR;ElGamal

中图分类号 TP393.08

文献标志码 A

0　引言

Introduction

无线局域网使用户能够真正实现随时、随地、随意地接入网络,然而,无线局域网的传输介质是开放的无线电波,这种开放性导致了无线局域网络面临窃听、欺骗、网络接管和篡改等多种安全威胁. 为此,IEEE 于 1997 年为 WLAN 制定了 802.11 标准,采用基于 RC4 算法的有线等效保密机制 WEP(Wired Equivalent Privacy)[1] 来增强其安全性. 但是,研究分析发现 WEP 无法有效地保证数据的机密性、完整性和对接入用户的身份认证.

要解决无线局域网的安全问题,需要在网络接入时实施严格的认证,并在通信过程中实现保密通信. 目前已出现了多种认证方式[2-3]. 本文针对无线局域网计算资源方面非对称的结构特点,设计了一个安全的认证方案,同时实现会话密钥的分配,为认证服务器 AS 配置计算量少的 Rabin-PSS-MR 签名的验证操作[4]、Rabin-OAEP 加密操作[5]和改进型 ElGamal 签名操作[6],为移动终端 STA 配置计算量较大的 Rabin-OAEP 解密操作和改进型 ElGamal 签名的验证操作,以此达到降低响应时延、提高网络效率的目的. 此外,为进一步节省通信带宽,将"发送公钥及相应证书"的传统公钥认证过程缩短为"仅发送公钥证书(而不发送公钥)"的精简模式,方法是采用具有消息恢复功能的 Rabin-PSS-MR 签名方案. 认证过程结束时,通信双方将同时得到一个共享的会话密钥以确保随后通信的保密性,实现认证功能与密钥分配功能的巧妙结合.

1　无线局域网认证结构

Authentication structure of WLAN

无线局域网的拓扑结构可分为两类:无中心拓扑结构和有中心拓扑结构[1],本文讨论如图 1 有中心拓扑结构的无线局域网.

要实现实体间的安全通信,要求移动终端 STA 在接入网络之前通过接入设备 AP 与认证服务器 AS 进行双向的认证. 只有通过认证才能继续进行保密通信. 在 802.1x 认证框架[7]中,认证过程主要涉及 3 个功能实体,即证书中心 CA、认证服务器 AS 和移动终端 STA.

1)证书中心 CA 负责为 STA 和 AS 颁发公钥证书. 证书是用消息恢复型 Rabin-PSS-MR 签名方案生成的,以使证书的验证工作量较小.

收稿日期 2009-07-04

资助项目 国家自然科学基金(60803135,90604009);综合业务网理论及关键技术国家重点实验室开放基金(ISN10-11);重庆市/信息产业部计算机网络与通信技术重点实验室开放基金(CY-CNCL-2008-01)

作者简介

刘佳,女,博士生,主要研究信息安全与密码学. liujia_1116@163.com

1　中山大学　信息科学与技术学院,广州,510275

2　仲恺农业工程学院,广州,510225

3　西安电子科技大学　综合业务网理论及关键技术国家重点实验室,西安,710071

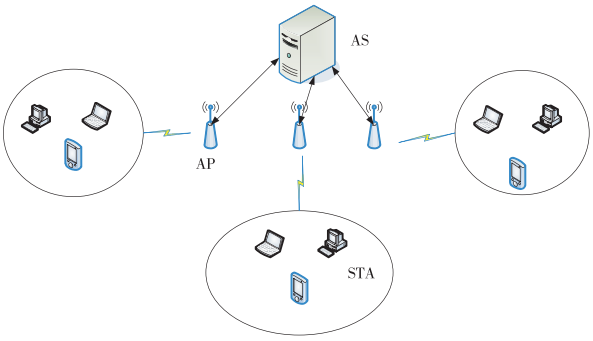


图 1　无线局域网系统网络模型

Fig. 1　Network model of WLAN system

2）认证服务器 AS 负责处理所有 STA 在任何时刻的接入认证请求,验证 STA 公钥证书及身份的合法性,并向 STA 提供 AS 公钥证书及身份的证明.

3）移动终端 STA 在接入网络前须向 AS 证明其公钥证书及身份的合法性,随后还要验证 AS 的公钥证书及身份.

STA 通常是桌面计算机或笔记本电脑,其计算资源相对充足;而 AS 虽然计算能力也不弱,但需要负责处理所有 STA 在任何时刻的接入认证请求,其计算任务相对繁重. 为了提高网络的运行效率,减小响应的时延,可以由 STA 承担认证过程中计算量较大的工作,尽量减少 AS 的工作量. 因此本文提出以下设计原则.

1）CA 发放公钥证书给 STA 和 AS,公钥证书的验证算法应该尽量简单.

2）STA 发送公钥证书给 AS 证明其合法性时,AS 验证工作量应该尽可能小;在验证 STA 身份时,AS 进行随机数加密操作,验证 STA 的解密能力,该过程计算量也应该尽可能小.

3）AS 向 STA 证明公钥证书及身份的合法性时,AS 发送公钥证书给 STA 证明其合法性,并发送签名给 STA 证明其身份,要求签名过程仅进行尽量少的运算.

2　基础密码算法

Basic cryptographic algorithms

为了实现认证服务器 AS 和移动终端 STA 的双向认证,为它们分别配置了不同的签名算法及加密算法,用以适应无线局域网特殊的非对称结构. 本节介绍认证方案中采用的密码算法:改进型 ElGamal 签名算法、Rabin-OAEP 加密算法、Rabin-PSS-MR 签名算法和 SMS4 分组加密算法[8].

2.1　改进型 ElGamal 签名算法

2.1.1　参数设置

取 p 为一个大素数,g 是 $\mathbf{Z}_p^*$ 的一个本原元,$x \in_R \mathbf{Z}_{p-1}$ 为私钥,$y = g^x \bmod p$ 为公钥,$m \in \mathbf{Z}_{p-1}$ 是待签名的消息.

2.1.2　签名生成

1）选取一个随机数 $r \in \mathbf{Z}_{p-1}$;

2）$V = g^r (\bmod p)$,$W = x(m + V) - r(\bmod p - 1)$. (W, V) 作为消息 m 的签名.

2.1.3　签名验证

收到签名 (W, V) 后,判断 $y^{(m+V)} = Vg^W \bmod p$ 是否成立. 若成立,则确认签名 (W, V) 有效,否则认定签名无效.

本文采用此改进型 ElGamal 签名算法是因为签名过程中的模幂运算 g^r 可预先计算,实时进行的只有模加和模乘运算,而无原始 ElGamal 签名方案[7]中的模逆运算. 这样,可以加快 AS 的运算速度,降低其响应时延.

2.2　Rabin-OAEP 加密算法

Rabin 原始算法无法抵抗自适应选择密文攻击. 为此,Bellare 和 Rogaway 提出最优非对称加密填充技术 OAEP (Optimal Asymmetric Encryption Padding)[5],采用随机化的消息填充技术,引入无碰撞的哈希函数,提供了可证明的安全性(附录 A). Rabin-OAEP 加密算法如图 2 所示.

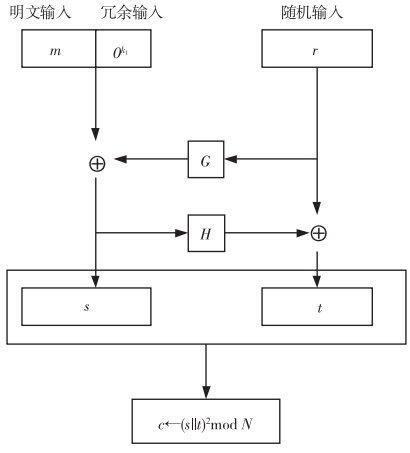


图 2　Rabin-OAEP 加密方案

Fig. 2　Rabin-OAEP encryption scheme

2.2.1　参数设置

运行密钥产生算法 $\mathrm{Gen}(1^k)$ 得到 $(N = pq, p, q, G, H, n, k_0, k_1)$,其中:$N = pq$ 是公钥;$p = q = 3 (\bmod 4)$ 是私钥;$|N| = k = n + k_0 + k_1$;2^{-k_0} 和 2^{-k_1} 为可忽略

的量;$H:\{0,1\}^{k-k_0}\rightarrow\{0,1\}^{k_0}$,$G:\{0,1\}^{k_0}\rightarrow\{0,1\}^{k-k_0}$是两个哈希函数;$n$ 是明文消息 m 的长度.

2.2.2 加密过程

对消息 $m\in\{0,1\}^n$ 进行加密,执行下列计算:

1) $r\leftarrow_U\{0,1\}^{k_0}$,$s\leftarrow(m\|0^{k_1})\oplus G(r)$,$t\leftarrow r\oplus H(s)$;

2) $c\leftarrow(s\|t)^2 \bmod N$. c 作为消息 m 的密文.

2.2.3 解密过程

收到密文 c 后,执行下列计算:

1) 利用私钥 p 和 q 计算

$s\|t\leftarrow q(q^{-1}\bmod p)c^{\frac{p+1}{4}}+p(p^{-1}\bmod q)c^{\frac{q+1}{4}}(\bmod N)$,其中 $|s|=n+k_1=k-k_0$,$|t|=k_0$;

2) $u\leftarrow t\oplus H(s)$,$v\leftarrow s\oplus G(u)$;

3) 若 $v=m\|0^{k_1}$ 输出消息 m,否则认为密文是无效的.

Rabin-OAEP 加密机制引入了哈希函数 G 和 H,其计算量相对于模幂和模逆等运算来说几乎可以忽略不计,但却能以如此小的代价获得如附录 A 所示的可证明安全性. 另外,AS 实施 Rabin-OAEP 加密操作时只须进行模平方运算和简单的哈希、异或运算,而将相对复杂的求平方根运算留给计算资源相对充裕的 STA,符合前述密码算法在认证方案中的配置原则.

2.3 Rabin-PSS-MR 签名算法

Rabin 原始签名函数属确定性算法,无法抵抗自适应选择消息攻击. Bellare 和 Rogaway 设计了 PSS(Probabilistic Signature Scheme)概率签名机制,并且能够实现消息恢复功能,形成 PSS-MR 方案. 图 3 给出了 Rabin-PSS-MR 签名方案的原理.

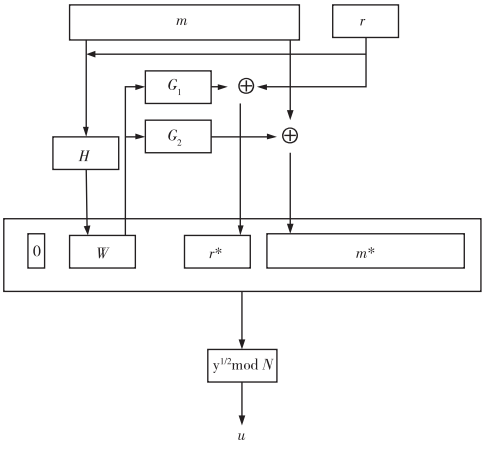


图 3 Rabin-PSS-MR 签名方案

Fig. 3 Rabin-PSS-MR signature scheme

2.3.1 密钥设置

运行密钥产生算法 $\mathrm{Gen}(1^k)$ 得到$(N=pq,p,q,G,H,n,k_0,k_1)$,其中:$N=pq$ 是公钥;$p=q=3(\bmod 4)$ 是私钥;$|N|=k=n+k_0+k_1+1$;2^{-k_0}和 2^{-k_1}为可忽略的量;$G:\{0,1\}^{k_1}\rightarrow\{0,1\}^{k-k_1-1}$,$H:\{0,1\}^*\rightarrow\{0,1\}^{k_1}$是两个哈希函数,进一步将 G 拆分成 $G_1\|G_2$,即 $G_1:\{0,1\}^{k_1}\rightarrow\{0,1\}^{k_0}$,$G_2:\{0,1\}^{k_1}\rightarrow\{0,1\}^n$;$n$ 是签名消息 m 的长度.

2.3.2 签名生成

欲对消息 $m\in\{0,1\}^n$ 进行签名,须执行下列计算:

1) $r\leftarrow_U\{0,1\}^{k_0}$,$w\leftarrow H(m\|r)$,$r^*\leftarrow G_1(w)\oplus r$,$m^*=G_2(w)\oplus m$;

2) $y\leftarrow 0\|w\|r^*\|m^*$;

3) 利用私钥 p 和 q 计算 $u\leftarrow q(q^{-1}\bmod p)y^{\frac{p+1}{4}}+p(p^{-1}\bmod q)y^{\frac{q+1}{4}}(\bmod N)$,$u$ 作为消息 m 的签名.

2.3.3 签名验证

收到签名 u 后,执行下列计算.

1) $y\leftarrow u^2 \bmod N$. 将 y 分段解释为 $b\|w\|r^*\|\gamma$,其中:b 是 k 比特 y 中的第一个比特;w 是后续的 k_1 比特;r^* 是在接下来的 k_0 比特;γ 是其余 n 比特.

2) $r\leftarrow G_1(w)\oplus r^*$,$m\leftarrow G_2(w)\oplus\gamma$.

3) 若 $H(m\|r)=w$ 且 $b=0$,则返回消息 m,并确认签名 u 有效,否则认定签名无效.

用 Rabin-PSS-MR 签名算法产生的公钥证书,根据文献[4],配置 1024 比特的证书和 767 比特的公钥,可以在公钥认证过程中只发送 1024 比特的证书而无须同时发送 767 比特的公钥——接收方仅利用证书(签名)就可以恢复出公钥消息,大大减少对通信带宽的要求. 而且证书的验证只须做模平方运算,可进一步减少 AS 的工作量. 此外,计算量几乎可忽略不计的哈希函数的引入同样能提供可证明的安全性(附录 B).

2.4 SMS4 分组加密算法

2006 年 1 月 6 日,中国国家密码管理局发布第 7 号公告,将用于我国无线局域网产品的加密标准确定为 SMS4 算法,这是国内官方公布的第一个商用密码算法. SMS4 是一个分组长度为 128 比特、密钥长度为 128 比特的分组密码算法,加密算法与密钥扩展算法都采用 32 轮非线性迭代结构,具体细节可参考文献[6].

SMS4 分组密码算法主要采用了异或、移位、查

表等操作,运行速度比公钥密码算法快许多,适用于海量数据的加解密. 这里用它来提供会话的保密性,关键问题是如何为通信的双方分配共享的会话密钥. 本文设计的认证方案能在成功认证的同时巧妙地实现会话密钥的分配.

3 无线局域网认证方案

WLAN authentication scheme

根据在第 2 节提出的设计原则,给出了 3 个认证实体的参数设置及其在认证过程中采用的密码算法,具体参数设置如表 1 所示. 图 4 给出了设计的无线局域网认证方案的交互过程.

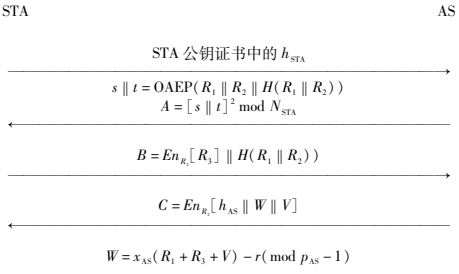


图 4 无线局域网认证方案

Fig. 4 WLAN authentication scheme

认证方案主要包括以下步骤.

1) STA 把公钥证书 h_{STA} 发送给 AS.

2) AS 利用 Rabin-PSS-MR 验证算法验证 STA 公钥证书的合法性;若认证成功,AS 选择两个随机数 R_1 和 R_2,计算其哈希函数值 $H(R_1 \| R_2)$,再利用 Rabin-OAEP 方案加密 R_1,R_2 和 $H(R_1 \| R_2)$,将加密结果 A 发送给 STA.

3) STA 利用 Rabin-OAEP 方案对 A 进行解密,恢复出 R_1 和 R_2,并检验其哈希值;如果解密成功,STA 选择一个随机数 R_3,以 R_2 为 SMS4 密钥加密 R_3 和 $H(R_1 \| R_2)$,即 $B = En_{R_2}[R_3 \| H(R_1 \| R_2)]$,将 B 发送给 AS.

4) 如果 AS 解密得到了正确的 $H(R_1 \| R_2)$,则可相信 STA 身份的合法性,并同时得到随机数 R_3;AS 利用其私钥 x_{AS} 和预计算值 $V = g^r \bmod p_{AS}$,计算改进型 ElGamal 签名 $W = x_{AS}(R_1 + R_3 + V) - r(\bmod p_{AS} - 1)$;并以 R_2 为 SMS4 密钥加密其证书 C_{AS} 中的 h_{AS}、W 和 V,即 $C = En_{R_2}[h_{AS} \| W \| V]$,将 C 发送给 STA.

5) STA 收到 AS 的加密消息 C 后,先用 R_2 解密恢复得到 C_{AS} 中的 h_{AS}、W 和 V;然后,用 Rabin-PSS-MR 算法验证证书的合法性. 若证书认证成功,STA 再检验 AS 的改进型 ElGamal 签名是否正确,即检验 $y_{AS}^{(R_1+R_3+V)} = Vg^W \bmod p_{AS}$ 是否成立. 如果成立,STA 就接受 AS 为合法服务器,双向认证结束.

认证结束后,STA 和 AS 可用 R_3 作为会话密钥加密双方后续的通信,以达到通信保密的目的.

本文的认证方案具有如下几个优势.

1) 由于采用消息可恢复的 Rabin-PSS-MR 概率签名作为公钥的证书,在 STA 向 AS 证明其公钥证书合法性时只需要发送公钥证书(签名)即可,而不需发送公钥(消息). 在 AS 向 STA 证明其公钥证书合法性时,情况类似. 通信过程中通信量减少了 $42.8\%\left(\frac{767}{(1\,024+767)}\right)$,这在很大程度上降低了对传输带宽的要求.

2) 由于 AS 负责处理所有 STA 在任何时刻的接入认证请求,其计算任务相对繁重;而 STA 的计算资

表 1 认证实体参数设置

Table 1 Setup of parameters for the entity to be certificated

实体	私钥	公钥	证书	密码运算
CA	Rabin 私钥:(p_{CA}, q_{CA}) $p_{CA} = q_{CA} = 3 \bmod 4$ $\lvert p_{CA} \rvert = \lvert q_{CA} \rvert = l_{CA}$	Rabin 公钥:N_{CA} $\lvert N_{CA} \rvert = 2l_{CA}$		Rabin-PSS-MR 签名
AS	ElGamal 私钥:x_{AS} $\lvert x_{AS} \rvert = l_{AS}$	ElGamal 公钥: $y_{AS} = g\hat{}(x_{AS}) \bmod p$ $\lvert y_{AS} \rvert = l_{AS}$	$C_{AS} = \{AS, y_{AS}, T_{AS}, h_{AS}\}$ $h_{AS} = y_{AS}{}^{1/2} \bmod N_{CA}$ $\lvert AS \rvert = l_{AS1}$, $\lvert T_{AS} \rvert = l_{AS2}$, $\lvert h_{AS} \rvert = 2l_{CA}$	Rabin-PSS-MR 签名的验证、Rabin-OAEP 加密、SMS4 解密、改进型 ElGamal 签名、SMS4 加密
STA	Rabin 私钥:(p_{STA}, q_{STA}) $p_{STA} = q_{STA} = 3 \bmod 4$ $\lvert p_{STA} \rvert = \lvert q_{STA} \rvert = l_{STA}$	Rabin 公钥:N_{STA} $\lvert N_{STA} \rvert = 2l_{STA}$	$C_{STA} = \{STA, N_{STA}, T_{STA}, h_{STA}\}$ $h_{STA} = N_{STA}{}^{1/2} \bmod N_{CA}$ $\lvert STA \rvert = l_{STA1}$, $\lvert T_{STA} \rvert = l_{STA2}$, $\lvert h_{STA} \rvert = 2l_{STA}$	Rabin-OAEP 解密、SMS4 加密、SMS4 解密、Rabin-PSS-MR 签名的验证、改进型 ElGamal 签名的验证

源相对充裕,故将方案中的认证方式设计成适合这种特点的非对称形式:由 STA 承担在认证过程中计算量较大的工作,减少 AS 的工作量,以提高网络的运行效率,减小响应的延时. 具体体现在以下 3 个方面:AS 验证 STA 公钥证书合法性时,进行的是 Rabin 签名的验证,只需做模平方这样一个简单的运算;AS 向 STA 发送挑战用以验证其是否持有公钥证书对应的私钥时,采用 Rabin 加密方案,也是只做一个模平方运算;由 AS 向 STA 实时证明自己身份时,采用改进型 ElGamal 签名方案,只需做模加和模乘运算.

3) 本方案没有像文献[10]一样直接用 Rabin 方案,这是因为 Rabin 函数是确定性算法,即 Rabin 签名算法输出的签名是由密钥(sk,pk)和 m 唯一确定的. 这种确定性使得选择消息攻击奏效,存在很大的安全隐患. 本文采用了具有消息恢复功能的 Rabin-PSS-MR 概率签名机制,虽然引入了两个哈希函数,但相对于公钥密码机制中的模幂和模逆等运算来说,其计算量几乎可以忽略不计. 然而,如此小的代价换来的是附录 B 的可证明安全性.

4) 认证协议运行结束时,通信双方获得了相同的会话密钥 R_3,即同时实现了密钥分配的功能.

综上所述,本文提出的基于消息可恢复型 Rabin-PSS-MR 概率签名机制的安全认证方案非常适合无线局域网的通信要求.

4 结束语

Concluding remarks

本文通过对无线局域网结构的分析,设计了一种基于公钥密码技术的认证方案. 该方案充分利用了 Rabin-PSS-MR 签名方案和 ElGamal 改进型签名方案中签名操作与验证操作的非对称性,实现了认证服务器 AS 与移动终端 STA 双向的高效认证及密钥分配,提高了网络的认证接入速度. 同时,Rabin-PSS-MR 签名方案使得公钥认证过程中只须发送证书而无须同时发送公钥,大大降低了对通信带宽的要求.

参考文献

References

[1] The LAN/MAN standards committee of the IEEE computer society. Wireless LAN medium access control and physical layer specification[S]. IEEE Std802.11—1997

[2] Chiba M,Dommety D,Eklund M,et al. Dynamic authorization extensions to remote authentication dial In user service(RADIUS)[S]. Request for Comments:5176,Network Working Group,2008

[3] Sterman B,Sadolevsky D,Schwartz D,et al. RADIUS extension for digest authentication[S]. Request for Comments:5090,Network Working Group,2008

[4] Bellare M,Rogaway P. The exact security of digital signatures: How to sign with RSA and Rabin[C]// Advances in Cryptology: Proceedings of EUROCRYPT'96, LNCS1070, Springer-Verlag, 1996:399-416

[5] Bellare M,Rogaway P. Optional asymmetric encryption[C]// Advances in Cryptology: Proceedings of EUROCRYPT'94, LNCS 950,Springer-Verlag,1994:92-111

[6] Harn L,Xu Y. Design of generalised ElGamal type digital signature schemes based on discrete logarithm[J]. IEEE Electronics letters,1994,30(24):433-439

[7] The LAN/MAN standards committee of the IEEE computer society. IEEE std802.1X-2001,IEEE standard for local and metropolitan area networks: Prot-based network access control[S]. IEEE New York,2001

[8] 国家密码管理办公室. 无线局域网产品使用的 SMS4 密码算法[EB/OL]. [2009-07-04]. http://www.oscca.gov.cn/doc/6/news_1106.htm,2006
National Password Management Office. SMS4 cipher algorithm used by WLAN products[EB/OL]. [2009-07-04]. http://www.oscca.gov.cn/doc/6/news_1106.htm,2006

[9] Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Trans Info Theory,1985,31(4):469-472

[10] 李志杰. 公钥密码技术在移动通信网络中的应用[J]. 中国科技信息,2005(8):15,33
LI Zhijie. Application of public key cipher technology in mobile communications network[J]. China Science and Technology Information,2005(8):15,33

附录 A:Rabin-OAEP 算法安全性证明

定理 1 假设分解大整数 $N=pq$ 是困难的(其中 p,q 为两个大素数),则 Rabin-OAEP 算法在自适应选择密文攻击下是安全的.

证明 等价地证明逆否命题"若 Rabin-OAEP 算法是不安全的,则大整数 N 可以分解".

Simulator 选择 α,计算 $y=\alpha^2 \bmod N$. 若能通过与 Adversary 的如下交互求得 $x_b \neq \pm\alpha$,使 $y=x_b^2 \bmod N$,则 Simulator 可分解大整数 $N=pq$.

为了与 Adversary 进行合理交互,Simulator 需仿真对 H 函数询问、G 函数询问和加密询问的应答,并分两个阶段进行应答.

1) 参数设置

运行密钥产生算法 $\mathrm{Gen}(1^k)$ 得到$(N=pq,p,q,G,H,n,k_0,k_1)$,其中 $N=pq$ 是公钥,$p=q=3 \pmod 4$ 是私钥;$|N|=k=n+k_0+k_1$;2^{-k_0}和2^{-k_1}为可忽略的量;$H:\{0,1\}^{k-k_0}\rightarrow\{0,1\}^{k_0}$,$G:\{0,1\}^{k_0}\rightarrow\{0,1\}^{k-k_0}$是两个哈希函数;$n$ 是明文消息 m 的长度.

2) 寻找阶段

a H 函数询问的应答仿真. Adversary 向 Simulator 询问 h_i 的 H 函数值,Simulator 随机选择 H_{h_i}发送给 Adversary,并把 H 函数的输入和输出对应关系存在列表 H_LIST;

b 数询问的应答仿真. Adversary 向 Simulator 询问 g_i 的 G 函数,Simulator 随机选择 G_{g_i}发送给 Adversary,并把 G 函数的输入和输出对应关系存在列表 G_LIST;

c 密询问的应答仿真. Adversary 发送明文 x_0,x_1 给 Simulator,Simulator 将挑战问题 y 作为 Adversary 的攻击密文提供给他,让其判断是 x_0 还是 x_1 对应的密文. 在 Simulator 控制 G_oracle 和 H_oracle 的情况下,任何消息(包括 x_0,x_1)都可能加密成 y,即只要对消息 x 选择随机数 r,控制 $G(r)=x\oplus s$ 和 $H(s)=r\oplus t$ 即可,既然这样,就没有理由怀疑 y 不是 x_0 或 x_1 的密文了,因此问题嵌入是合理的.

3) 猜测阶段

a H 函数询问的应答仿真. Adversary 向 Simulator 询问 h_i 的 H 函数值,Simulator 随机选择 H_{h_i}发送给 Adversary,并把 H 函数的输入

和输出对应关系存在列表 H_LIST,同时遍历 G_LIST,计算 $y_j=(h_i \| H_{h_i}\oplus g_j)^2, j=1,2,\cdots,\Lambda$,如果存在 y_j 使 $y=y_j$,则令 $w=h_i \| H_{h_i}\oplus g_j$,按照 Rabin-OAEP 解密过程,将 w 分段解释成 $s \| t$, $|s|=n+k_1=k-k_0$, $|t|=k_0$;$u\leftarrow t\oplus H(s)$,$v\leftarrow s\oplus G(u)$;若 $v=x_b \| 0^{k_1}$,输出消息 x_b,如果 $x_b\neq\pm\alpha$,算法 Simulator 就可以分解大整数 $N=pq$:由 $x_b^2=\alpha^2 \bmod N$ 有 $\alpha+x_b \mid N$ 和 $\alpha-x_b \mid N$.

b G 函数询问的应答仿真. Adversary 向 Simulator 询问 g_i 的 G 函数,Simulator 遍历 H_LIST,计算 $y_j=(h_j \| H_{h_j}\oplus g_i)^2, j=1,2,\cdots,\Lambda$. 如果存在 y_j 使 $y=y_j$,则令 $w=h_j \| H_{h_j}\oplus g_i$,按照 Rabin-OAEP 解密过程,可得消息 x_b,如果 $x_b\neq\pm\alpha$,算法 Simulator 就可以分解大整数 $N=pq$:由 $x_b^2=\alpha^2 \bmod N$ 有 $\alpha+x_b \mid N$ 和 $\alpha-x_b \mid N$. 同时计算 $G_{g_i}=x_b\oplus h_j$,$b\leftarrow\{0,1\}$,并发送 G_{g_i} 给 Adversary;如果不存在 y_j 使 $y=y_j$,Simulator 随机选择 G_{g_i} 发送给 Adversary,并把 G 函数的输入和输出对应关系存在列表 G_LIST;

Adversary 以大于 1/2 的概率发送攻击密文 y 对应的明文 x_b,$b\leftarrow\{0,1\}$ 给 Simulator,则有理由相信,Adversary 会以某种技巧(概率大于 1/2)去对 x_0 和 x_1 进行加密尝试,其中 Adversary 可能用了一些随机数 r,向控制 G_oracle 和 H_oracle 输出的 Simulator 提出 r 的 G 询问和 s 的 H 询问. 其提问和回答均被 Simulator 记录. 当 Adversary 提供 b 的回答时,虽然他不知道 Adversary 用了哪时的(r,s)取得的成功,但 Simulator 相信其已经尝试成功,并且他相信(r,s)必被询问并记录过,因此他只需要逐一尝试其记录即可.

附录 B:Rabin-PSS-MR 签名算法安全性证明

定理 2 假设分解大整数 $N=pq$ 是困难的(其中 p,q 为两个大素数),则 Rabin-PSS-MR 算法在自适应选择消息攻击下是不可伪造的.

证明 等价地证明逆否命题"若 Rabin-PSS-MR 算法是不安全的,则大整数 N 可以分解".

Simulator 选择 α,计算 $y=\alpha^2 \bmod N$. 若能通过与 Adversary 的如下交互求得 $\beta\neq\pm\alpha$,使 $y=\beta^2 \bmod N$,则 Simulator 可分解大整数 $N=pq$.

为了与 Adversary 进行合理交互,Simulator 需仿真对签名询问、H 函数询问和 G 函数询问的应答.

1) 密钥设置

运行密钥产生算法 $\mathrm{Gen}(1^k)$ 得到$(N=pq,p,q,G,H,n,k_0,k_1)$,其中 $N=pq$ 是公钥,$p=q=3 \pmod 4$ 是私钥;$|N|=k=n+k_0+k_1+1$;2^{-k_0}和2^{-k_1}为可忽略的量;$G:\{0,1\}^{k_1}\rightarrow\{0,1\}^{k-k_1-1}$,$H:\{0,1\}^*\rightarrow\{0,1\}^{k_1}$是两个哈希函数,进一步将 G 拆分成 $G_1 \| G_2$,即 $G_1:\{0,1\}^{k_1}\rightarrow\{0,1\}^{k_0}$,$G_2:\{0,1\}^{k_1}\rightarrow\{0,1\}^n$;$n$ 是签名消息 m 的长度.

2) 签名询问

a Adversary 向 Simulator 询问消息 m_i 的签名,Simulator 任选 k_0 比特的随机数 r_i;

b 如果存在 $j:j<i, r_j=r_i$,则仿真终止;

c 随机选择 s_i,计算 $y_i=s_i^2 \bmod N$ 满足最高比特位为 0. 把 y_i 写成 $y_i=0 \| w_i \| r_i^* \| m_i^*$,其中 w_i 是 k_1 比特,r_i^* 是 k_0 比特,m_i^* 是最后 $k-k_0-k_1-1$ 比特. 令 $H(m_i \| r_i)=w_i$,$G_1(w_i)=r_i\oplus r_i^*$,$G_2(w_i)=m_i\oplus m_i^*$,$G(w_i)=G_1(w_i) \| G_2(w_i)$,把 H 函数和 G 函数输入和输出对应关系分别存在列表 H_LIST0,G_LIST0 中;

d 如果存在 $j:j<i$,使 $w_j=w_i$,则仿真终止;

e 把 s_i 当作消息 m_i 的签名发送给 Adversary,同时 Simulator 保存(m_i,r_i,s_i,y_i);

f Adversary 在接收到 m_i 的签名 s_i 后,如果要进行验证,首先求 $y_i=s_i^2=0 \| w_i \| r_i^* \| m_i^*$,验证 $w_i=H(m_i \| r_i)$,其中 $r_i=G_1(w_i)\oplus r_i^*$,$m_i^*=G_2(w_i)\oplus m_i$,若等式成立,说明 m_i 的签名就是 s_i,其中 H 函数和 G 函数都要去询问 Simulator.

3) H 函数询问的应答仿真

a Adversary 向 Simulator 询问 $m_i \| r_i$ 的 H 函数值,Simulator 搜索 H_LIST0 列表,如果存在 $j<i$,使 $m_j \| r_j=m_i \| r_i$,就从列表 H_LIST0 中查找此 H 函数输入对应的输出发送给 Adversary;

b 如果不存在 $j<i$,使 $m_j \| r_j=m_i \| r_i$,则随机选择 s_i,计算 $y_i=s_i^2\cdot y=0 \| w_i \| r_i^* \| m_i^*$,令 $w_i=H(m_i \| r_i)$;

c 如果存在 $j<i$,使 $w_j=w_i$,则仿真终止. 若不存在 $j<i$,使 $w_j=w_i$,则令 $G_1(w_i)=r_i\oplus r_i^*$,$G_2(w_i)=m_i\oplus m_i^*$,$G(w_i)=G_1(w_i) \| G_2(w_i)$,把 H 函数和 G 函数输入和输出对应关系分别存在列表 H_LIST1,G_LIST1,同时在 Simulator 保存(m_i,r_i,s_i,y_i);

d 最后发送 $w_i=H(m_i \| r_i)$ 给 Adversary 作为 $m_i \| r_i$ 的 H 函数值.

e G 函数询问的应答仿真.

Adversary 向 Simulator 询问 w_i 的 G 函数,Simulator 搜索列表 G_LIST0 和 G_LIST1,如果存在 $j<i$,使 $w_j=w_i$,直接返回对应的输出. 否则随机选择 $k-k_1-1$ 比特的 α,使 $G(w_i)=\alpha$,发送 α 给 Adversary 作为 w_i 的 G 函数值.

若 Adversary 能以不可忽略的概率伪造有效 Rabin-PSS-MR 消息签名对(m,s),则它应该能通过验证. Simulator 计算 $Y=s^2=0 \| w \| r^* \| m^*$,$r=r^*\oplus G_1(w)$,以不可忽略的概率在列表中找到$(m,r,w,r^*,m^*)=(m_i,r_i,w_i,r_i^*,m_i^*)$,即 $Y=s^2=0 \| w \| r^* \| m^*=s_i^2\cdot y=0 \| w_i \| r_i^* \| m_i^*$,亦即 $s^2=s_i^2\cdot y$,则 $y=\left(\frac{s}{s_i}\right)^2$,设 $\beta=\frac{s}{s_i}$,如果 $\beta\neq\pm\alpha$,算法 Simulator 就可以分解大整数 $N=pq$:由 $\beta^2=\alpha^2 \bmod N$ 有 $\alpha+\beta \mid N$ 和 $\alpha-\beta \mid N$. 证毕.

WLAN authentication scheme based on message-recovery Rabin-PSS

LIU Jia[1,2] WEI Baodian[1,3] DAI Xianhua[1]

1 School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510275

2 ZhongKai Institute of Agricultural Engineering, Guangzhou 510225

3 State Key Lab of Integrated Service Networks Theory and Key Technology, Xidian University, Xi'an 710071

Abstract Taking the asymmetric architecture of the wireless local area network into consideration, we propose an identity authentication scheme based on the public key cipher technology, where secret session-key sharing is accompanied with the successful authentications. The authentication sever AS and the mobile terminals STAs are properly configured with different workloads of signature generations and signature verifications in Rabin-PSS-MR scheme and the improved ElGamal signature scheme, aiming to greatly enhance the network's response efficiency. The message recovery function of the Rabin-PSS-MR scheme has reduced the transmission workload sharply since the public keys are not necessary to be transmitted in this scheme, which has saved a great deal of communication bandwidth.

Key words WLAN; authentication; Rabin-PSS-MR; ElGamal