基于矢积的远程口令鉴别方案

谭凯军, 何 晨, 诸鸿文
(上海交通大学电子工程系, 上海 200030)

摘 要: 本文提出了一种基于矢积的远程口令鉴别方案. 本方案中, 合法用户在智能卡初始化时可以自由地选取自己的口令. 用户利用智能卡以及口令便可成功地登录到远程系统. 根据分析, 攻击者不能从公开或传送的信息中获得用户秘密信息, 也不能冒充别的合法用户. 此外, 本方案还能抵抗登录请求的重播. 本方案所需的计算量大大地小于 G-H 方案.

关键词: 远程口令鉴别; 矢别; 登录请求; 时间标志; 智能卡
中图分类号: TP393 文献标识码: A 文章编号: 0372-2112 (2000) 02-0028-03

Remote Scheme for Password Authentication Based on Cross-Product

TAN Kai-jun, HE Chen, ZHU Hong-wen
(*Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai* 200030, *China*)

Abstract: A remote password authentication scheme based on cross-product is proposed in this paper. In this scheme, any legal user can freely choose his own password in the card initialization phase. Using his password and smart card, he can then log into the remote system successfully. According to the analysis, intruders can not obtain any secret information from the public information or transmitted messages and impersonate another legal user. In addition, this scheme can withstand the attack of replaying previously intercepted log in requests. The amount of computation in this scheme are smaller than that in G-H scheme.

Key words: remote password authentication; cross-product; login request; time stamp; smart card

1 引言

随着科学技术的迅速发展, 人们越来越依靠网络来与远端通信并协同完成工作. 网络为人们的远程协作提供了方便, 然而由于传输网的非安全的特点, 使得信息很容易被攻击者访问或截取.

达到口令鉴别最传统的方法是在主机中存放一张口令表 (包含用户识别符 ID 以及口令 PW), 可是一旦口令表被攻击, 那么所有的口令均被揭露. 于是人们将口令加密后存储在口令表中[1,2], 但这些方案不能抵抗重播攻击. Lamport[3] 提出了一种可以抵抗重播攻击的方案, 然而当存储在主机的被加密的口令一旦遭到攻击者的修改, 方案也是不安全的. 为了避免这种威胁, Chang 和 Wu[4] 提出了一种在智能卡中实现的远程口令鉴别方案, 但 Chang 和 Liah 在文[5] 中指出该方案是不安全的. Chang 和 Hwang[6] 提出了另一个在智能卡中实现的远程口令鉴别方案, 是基于离散对数问题的, 但它需要系统为每个用户产生口令, 这种情况是不合理且不安全的. 文[7] 中, Wu 提出了一种基于几何问题的远程口令鉴别方案, 该方案中, 用户能自己选择口令.

本文我们提出了一种在智能卡中实现的基于矢积的远程口令鉴别方案, 用户能自己选择口令并且计算量大大小于 Chang 和 Hwang 方案. 文章的组织如下: 第二部分简单介绍 Chang 和 Hwang 方案[6]. 第三部分介绍本文提出的方案. 第四部分是安全性及性能分析. 第五部分是结论.

2 Chang 和 Hwang 远程口令鉴别方案

p 是一个大素数, α 是 $GF(p)$ 中的本原元. 系统选择一秘密的 $n\times n$ 的非奇异矩阵: $\boldsymbol{K}=\begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ k_{n1} & k_{n2} & \cdots & k_{nn} \end{bmatrix}$, n 是一个正整数, $k_{ij}\in GF(p)(i,j=1,2,\cdots,n)$. 此外, 选一单向函数 $f(\cdot)$ 以及一伪随机数产生函数 $g(\cdot)$. p, α, $f(\cdot)$ 公开, $g(\cdot)$, K 由系统秘密保存. 接着系统计算: $\boldsymbol{PK}=\begin{bmatrix} pk_{11} & pk_{12} & \cdots & pk_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ pk_{n1} & pk_{n2} & \cdots & pk_{nn} \end{bmatrix}$, 其中 $pk_{ij}=\alpha^{k_{ij}} \bmod p\ (1\le i,j\le n)$.

一般的, 远程口令鉴别方案分成三个阶段:

2.1 智能卡初始化阶段

系统中有一受信赖的智能卡初始化中心 CIC. 当一新用户 u_i 注册时, 由 CIC 向其分发智能卡.

(1) u_i 递交其身份识别符 $\boldsymbol{ID}_i=(id_{i1}, id_{i2}, \cdots, id_{in})$;

收稿日期: 1998-10-10; 修订日期: 1999-03-11

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

(2)CIC 计算:

$$\boldsymbol{PW}_i=\begin{bmatrix}pw_{i1}\\pw_{i2}\\\vdots\\pw_{in}\end{bmatrix}=\begin{bmatrix}k_{11}&k_{12}&\cdots&k_{1n}\\\vdots&\vdots&\vdots&\vdots\\k_{n1}&k_{n2}&\cdots&k_{nn}\end{bmatrix}^{-1}\begin{bmatrix}g(id_{i1})\\g(id_{i2})\\\vdots\\g(id_{in})\end{bmatrix},\ \boldsymbol{K}^{-1}\text{是}\ \boldsymbol{K}$$

的逆矩阵;

(3)将一张包含$(\boldsymbol{PK}, f(\cdot))$的智能卡分发给 u_i, 而 $\boldsymbol{PW}_i$ 作为 u_i 的口令通过秘密渠道传给 u_i.

2.2　登录阶段

(1)当 u_i 想登录入远程系统时, 先将智能卡插入本地一个终端, 并输入 $\boldsymbol{PW}_i$; (2)智能卡随机选择一个整向量 $\boldsymbol{V}=(v_1, v_2, \cdots, v_n)$, $v_i\in GF(p)$; (3)计算向量 $\boldsymbol{S}=(s_1, s_2, \cdots, s_n)$, $s_m=\prod_{j=1}^{n} p k_{mj}^{v_j} \bmod p$, $m=1, 2, \cdots, n$; (4)计算 $\boldsymbol{PW}'_i=(pw'_1, pw'_2, \cdots, pw'_n)=\boldsymbol{PW}_i+(V* f(S, T)(\bmod p-1))$, T 是当时的时间标志; (5)组成登录请求 $\boldsymbol{R}=(ID_i, PW'_i, S, T)$, 向远程系统发送.

2.3　鉴别阶段

假设远程系统接到请求的时间为 T^*, 那么通过以下过程来验证请求:

(1)验证 $\boldsymbol{ID}_i$ 是否正确, 不正确的话拒绝此次登录请求;

(2)计算 T^*-T, 如果 $T^*-T>\Delta T$(ΔT 是允许的最大时间间隔), 那么表示超时, 拒绝此次登录;

(3)计算: $\boldsymbol{Q}_i=\begin{bmatrix}q_1\\q_2\\\vdots\\q_n\end{bmatrix}=\begin{bmatrix}k_{11}&k_{12}&\cdots&k_{1n}\\\vdots&\vdots&\vdots&\vdots\\k_{n1}&k_{n2}&\cdots&k_{nn}\end{bmatrix}^{-1}\begin{bmatrix}pw'_1\\pw'_2\\\vdots\\pw'_n\end{bmatrix}$

(4)如果: $\alpha^{q_j}\equiv\alpha^{g(id_{ij})}* s_j^{f(S,T)}(\bmod p)$, $j=1, 2, \cdots, n$, 那么接受此次登录请求, 否则拒绝.

3　本文提出的方案

本文所提出的方案是基于矢积的. 首先介绍有关的数学根据:

定义 **1**[8]　$\boldsymbol{V}_1=(v_{11}, v_{12}, v_{13})$, $\boldsymbol{V}_2=(v_{21}, v_{22}, v_{23})$ 是两个线性无关的 3 维的行向量, $\boldsymbol{V}_1$ 和 $\boldsymbol{V}_2$ 在 $GF(p)$ 上的矢积定义为:

$$(\boldsymbol{V}_1\times\boldsymbol{V}_2)(\bmod p)=\left(\begin{vmatrix}v_{12}&v_{13}\\v_{22}&v_{23}\end{vmatrix},\begin{vmatrix}v_{13}&v_{11}\\v_{23}&v_{21}\end{vmatrix},\begin{vmatrix}v_{11}&v_{12}\\v_{21}&v_{22}\end{vmatrix}\right)(\bmod p)$$

, $|M|$ 表示矩阵 $\boldsymbol{M}$ 的行列式.

定义 **2**[8]　让 $\boldsymbol{V}=(v_1, v_2, v_3)$ 是三维的行向量, 且 $v_1\neq 0$, $\boldsymbol{V}$ 在 $GF(p)$ 上的归一化定义为:

$$N(\boldsymbol{V})=(v_2\cdot v_1^{-1}, v_3\cdot v_1^{-1})(\bmod p)$$

v_1^{-1} 是 v_1 在 $GF(p)$ 中的逆.

定理 **1**[8]　让 $\boldsymbol{V}_1$ 和 $\boldsymbol{V}_2$ 是两个线性无关的 3 维行向量, $\boldsymbol{A}$ 是一个 $m\times 2$ 矩阵($m\geq 2$), 并且任何两个行向量都是线形无关的. $\boldsymbol{A}$ 中任何元素均为非 0, 如果: $\begin{pmatrix}k_1&k_2&\vdots&k_m\end{pmatrix}^T=A\begin{pmatrix}\boldsymbol{V}_1&\boldsymbol{V}_2\end{pmatrix}^T(\bmod p)$, 那么 $k_i\times W=C(\boldsymbol{V}_1\times\boldsymbol{V}_2)(\bmod p)$, $i=1, 2, \cdots, m$. C 是一个常量, $W=\boldsymbol{V}_1$ 或 $W=\boldsymbol{V}_2$.

由定理 1 可以得出推论: $\boldsymbol{V}_1$ 和 $\boldsymbol{V}_2$ 是两个线性无关的 3 维行向量, k_i 和 k_j 如定理 1 中所定义, 如果 $N(k_i\times\boldsymbol{N}_2)$, $N(k_j\times\boldsymbol{V}_2)$, $N(\boldsymbol{V}_1\times\boldsymbol{V}_2)$ 是符合定理 1 的, 那么:

$N(k_i\times\boldsymbol{V}_i)=N(k_j\times\boldsymbol{V}_1)=N(\boldsymbol{V}_1\times\boldsymbol{V}_2)$, $N(k_i\times\boldsymbol{V}_2)=N(k_j\times\boldsymbol{V}_2)=N(\boldsymbol{V}_1\times\boldsymbol{V}_2)$.

下面介绍以上的推论如何应用在所提出的方案中. 假设系统中也有一个智能卡初始化中心 CIC, 它的任务就是为用户分发智能卡.

p 是一个大素数, α 为模 p 的起源元, $f(\cdot)$, $g(\cdot)$ 的意义为 Chang 和 Hwang 方案中的相同. 系统随机选取两个线性无关的 3 维的行向量 $\boldsymbol{V}_1=(v_{11}, v_{12}, v_{13})$, $\boldsymbol{V}_2=(v_{21}, v_{22}, v_{23})$. $\boldsymbol{V}_1$、$g(\cdot)$秘密保存, 而 α、p、$\boldsymbol{V}_2$ 公开. 选择一个 $n\times 2$ 矩阵 $\boldsymbol{A}$(n 为系统中预定注册人数), $\boldsymbol{A}$ 中的任何两个行向量都是线性无关的, 这些行向量将分配给不同的用户, 当行向量全部分配完后, 再随机选取一个与 $\boldsymbol{A}$ 中所有行向量都线性无关的二维行向量分配给新用户, 将其加入 $\boldsymbol{A}$, 并改变 $\boldsymbol{A}$ 为 $(n+1)\times 2$ 矩阵. 将方案的实现分成三个阶段:

(1)智能卡初始化阶段　当一新用户 u_i 注册时, 由 CIC 向其分发智能卡. u_i 递交其身份识别符 $\boldsymbol{ID}_i=(id_{i1}, id_{i2})$ 以及 $f(\boldsymbol{PW}_i)$, $\boldsymbol{PW}_i$ 是用户 u_i 为自己选取的口令;

(a)CIC 从 $\boldsymbol{A}$ 中选取一未曾分配的 2 维行向量 $\boldsymbol{A}_i=(a_{i1}, a_{i2})$, $a_{i1}\neq 0$, $a_{i2}\neq 0$;

$$(b)\text{CIC 计算: } k_i=(a_{i1}, a_{i2})\cdot\begin{pmatrix}V_1\\V_2\end{pmatrix}(\bmod p)\qquad(1)$$

$$PW1_i=N(k_i\times\boldsymbol{V}_2)\begin{pmatrix}g(id_{i1})\\g(id_{i2})\end{pmatrix}\oplus f(\boldsymbol{PW}_i)(\bmod p)\qquad(2)$$

($\oplus$是将 10 进制数转换成二进制数进行异或, 然后再将二进制结果转换成 10 进制数.)

(c)CIC 将智能卡传递给 u_i, 卡中包含$(PW1_i, k_i, f(\cdot))$.

(2)登录阶段

(a)当 u_i 想登录入远程系统时, 他先将智能卡插入本地一个终端, 并输入 $\boldsymbol{PW}_i$;

$$(b)\text{智能卡计算 } PW2_i=\boldsymbol{PW}1_i\oplus f(\boldsymbol{PW}_i)(\bmod p)\qquad(3)$$

$$PW3_i=\alpha^{N(k_i\times V_2)\cdot(f(PW2_i),f(T))}(\bmod p)\qquad(4)$$

"$\cdot$" 表示矢量内积: $(x_1, x_2)\cdot(y_1, y_2)=x_1y_1+x_2y_2(\bmod p-1)$, T 为当时的时间标志;

(c)组成登录请求 $R=(PW3_i, T, \boldsymbol{ID}_i)$, 向远程系统发送.

(3)鉴别阶段　假设远方收到 R 的时间为 T^*, 那么通过以下过程来验证请求:

(a)验证 $\boldsymbol{ID}_i$ 是否正确, 不正确的话拒绝此次登录请求;

(b)计算 T^*-T, 如果 $T^*-T>\Delta T$(ΔT 是允许的最大时间间隔), 那么表示超时, 拒绝此次登录;

$$(c)\text{计算: } Q=N(\boldsymbol{V}_1\times\boldsymbol{V}_2)\begin{pmatrix}g(id_{i1})\\g(id_{i2})\end{pmatrix}(\bmod p)\qquad(5)$$

$$Z=\alpha^{N(V_1\times V_2)\cdot(f(Q),f(T))}(\bmod p)\qquad(6)$$

如果 $PW3_i=Z$, 那么表示鉴别成功, 否则拒绝登录.

证明　$\boldsymbol{PW}3_i=Z$:

因为 $\boldsymbol{PW}2_i=\boldsymbol{PW}1_i\oplus f(\boldsymbol{PW}_i)(\bmod p)$

$$=N(k_i\times\boldsymbol{V}_2)\begin{pmatrix}g(id_{i1})\\g(id_{i2})\end{pmatrix}(\bmod p),$$

© 1994-2016 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

$$Q = N(\boldsymbol{V}_1 \times \boldsymbol{V}_2)\begin{pmatrix} g(id_{i1}) \\ g(id_{i2}) \end{pmatrix} \pmod p,$$

而 $N(\boldsymbol{V}_1 \times \boldsymbol{V}_2) = N(k_i \times \boldsymbol{V}_2)$,

所以 $\boldsymbol{PW}2_i = Q, f(\boldsymbol{PW}2_i) = f(Q)$, $\boldsymbol{PW}3_i = Z$.

例子:

假设取 $\boldsymbol{V}_1 = (1, 2, 3)$, $\boldsymbol{V}_2 = (4, 5, 6)$, $p = 13$, $\alpha = 7$,

$$\boldsymbol{A} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}.$$

CIC 将给 u_1 分发智能卡, 设 $\boldsymbol{ID}_1 = (1, 3)$, $g(id_{11}) = 4$, $g(id_{12}) = 7$, $f(\boldsymbol{PW}_1) = 11$, 那么 CIC 从 $\boldsymbol{A}$ 中选取一行向量 $\boldsymbol{A}_1 = (1, 2)$, 利用式(1)计算出 $\boldsymbol{k}_1 = (9, 12, 2)$, 再通过式(2)求得:

$$\boldsymbol{PW}1_1 = N(k_1 \times V_2)\begin{pmatrix} 4 \\ 7 \end{pmatrix} \oplus f(\boldsymbol{PW}_1) \pmod p = (2, 1)\begin{pmatrix} 4 \\ 7 \end{pmatrix} \ominus 11 \pmod p = (1111)_2 \ominus (1011)_2 \pmod p = (0100)_2 = 4$$

所以卡中包含有$(4, (9, 12, 2), f(\cdot))$.

当 u_1 要访问远程系统时, 他先将智能卡插入本地一个终端, 并输入 $\boldsymbol{PW}_1$. 智能卡利用式(3)计算 $\boldsymbol{PW}2_1 = (0100)_2 \oplus (1011)_2 = (1111)_2 = 2 \pmod{13}$, $f(\boldsymbol{PW}2_1) = 3$, 假设当时的时间为 T, $f(T) = 5$, 再利用式(4)计算 $\boldsymbol{PW}3_1 = 7^{(2,1)\cdot(3,5)} \bmod 13 = 2$, 所以 $R = (2, T, (1, 3))$. 假设远方收到 R 的时间为 T^*, 那么先验证 $\boldsymbol{ID}_1 = (1, 3)$ 是否正确, 不正确的话拒绝此次登录请求. 再计算 $T^* - T$, 如果 $T^* - T > \Delta T$ (ΔT 是允许的最大时间间隔), 那么表示超时, 拒绝此次登录. 利用计算式(5)计算

$$Q = (2, 1)\begin{pmatrix} 4 \\ 7 \end{pmatrix} \pmod{13} = 2, f(2) = 3,$$

$$Z = 7^{(2,1)\cdot(3,5)} \pmod{13} = 2.$$

所以 $\boldsymbol{PW}3_1 = Z$, 鉴别成功, 否则拒绝登录.

4 安全性及性能分析

正规化地验证一个密码算法的安全性是较困难的[7]. 本文从本方案中可能遭到的攻击来讨论它的安全性.

(1)G-H 方案中口令是由 CIC 分配给用户的, 这种情况不合理, 而且不安全. 因为分配的口令通常难以记住, 用户就需要用某种方法来记录这个口令, 那么就有很大的可能泄露这个口令. 另外, CIC 知道所有用户的口令, 如果 CIC 不诚实的话, 那么所有的口令都有可能暴露. 而本文的方案中用户可以自己选择口令, 而且口令是用单向函数的形式 $f(\boldsymbol{PW}_i)$ 传送给 CIC 的, 并没有向 CIC 暴露其真实口令, 安全性更好. CIC 如果想要获得真实口令, 往往需要解单向函数, 而这是不可能的. 单向函数的定义是如果有 x, 很容易求得 $y = f(x)$, 但是知道 y, 却很难求得 x. 登录验证过程中更是用到 $f(\boldsymbol{PW}_i)$ 的变化形式, 除了用户以外的任何人都无法知道用户的真正口令.

(2)由于时间标记的作用可以抵抗登录请求的重播, 即使攻击者可以改变 R 中的 T, 但是它无法改变 $PW3_i$. 这可以分两种情况: (a) 如果它是远程系统的合法用户 u_j, 即它有合法的 k_j, 那么它能计算 $N(k_j \times V_2)$, 但因为它不知道系统的 $g(\cdot)$, 所以即使利用 ID_i, 也无法计算出正确的 $N(k_i \times V_2)\begin{pmatrix} g(id_{i1}) \\ (id_{i2}) \end{pmatrix} \pmod p = \boldsymbol{PW}2_i$, 所以即使它改变新时间为 T', 却不能正确计算出改变时间后的 $PW3'_i$. (b)如果它不是远方系统的合法用户, 那么它既没有合法的 k_j, 也不知 $g(\cdot)$, 根本无法生成改变时间后的 $\boldsymbol{PW}3'_i$.

(3)任何攻击者想伪装成合法用户 u_i 登录都是不可以的, 首先他没有智能卡, 即使获得了智能卡, 但不知道正确的口令也不行. 如果口令不正确, 那么 $\boldsymbol{PW}2_i$, $\boldsymbol{PW}3_i$ 都是不正确的, 鉴别也得不到正确的结果.

(4)任何人从传送的信息 $\boldsymbol{PW}3_i$ 不能得到任何有关登录用户 u_i 的秘密信息, 即从 $\boldsymbol{PW}3_i$ 中不能得到 $N(k_i \times \boldsymbol{V}_2) \cdot (f(\boldsymbol{PW}2_i), f(T))$, 因为这相当于解离散对数的难度, 进而, 他也根本不可能求得 $k_i, f(\boldsymbol{PW}2_i), PW2_i$.

(5)本方案的计算量较 G-H 方案少得多.

(a)初始化时, G-H 方案需要 n^2 次模乘, 本方案是 16 次模乘. (b)登录请求时, G-H 方案需要 n^2 次模乘, n^2 次模的幂乘, 本方案是 10 次模乘, 1 次模的幂乘, 2 次 $GF(p)$ 上求逆运算. (c)验证时, G-H 方案需要 $3n$ 次模的幂乘, $n^2 + n$ 次模乘, 本方案是 12 次模乘, 1 次模的幂乘, 2 次 $GF(p)$ 上求逆运算. 但因为 $N(\boldsymbol{V}_1 \times \boldsymbol{V}_2)$ 可以预先计算好, 所以模乘次数可以减少到 4 次.

5 结论

本文提出了一种基于矢积的远程口令鉴别方案. 本方案中, 合法用户在智能卡初始化时可以自由地取自己的口令. 用户利用智能卡以及口令便可成功地登录到远程系统. 根据分析, 攻击者不能从公开或传送的信息中获得用户的秘密信息, 也不能冒充别的合法用户. 此外, 本方案还能抵抗登录请求的重播. 本方案所需的计算量大大地小于 G-H 方案.



谭凯军 1972 年生. 1994 年毕业于长春光学精密机械学院计算机科学系, 获工学学士学位. 1997 年毕业于南京理工大学计算机科学系, 获工学硕士学位. 现就读于上海交通大学电子工程系, 为在读博士. 主要研究方向为计算机和通信网络安全, 密码学.



何 晨 1982 年获东南大学无线电系获工学士, 1985 年获该校工学硕士. 1994 年获日本国立德岛大学工学博士. 1985 年加入东南大学电子工程系, 1990 年赴日本德岛大学做访问学者, 现为上海交通大学电子工程系副教授. 主要研究方向为神经网络与智能信息处理, 信息论与编码, 平流层通信.

(下转第 100 页)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

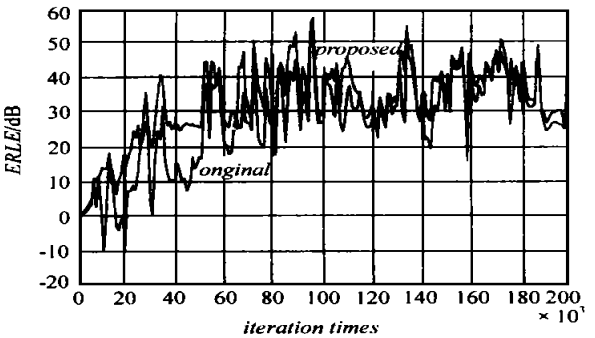


图 5 回声衰减增益的比较

法,而在自适应横向滤波部分采用 LMS 算法,得到了比全部采用 LMS 算法更好的声回波抑制性能.从逆谱滤波的观点对稳定性问题做出合理的解释,并提出一种有效方法,解决了一般快速 RLS 算法固有的稳定性问题.将算法广泛用于不同的 LRM 系统和不同的语音激励加以考查值得进一步研究.

参考文献

[1] T. Petillon et al. The fast Newton transversal filter: An efficient scheme for acoustic echo cancellation in mobile radio. IEEE Trans. Signal Processing, 1994, 42(3): 509~518

[2] B. Farhang-Boroujeny. Fast LMS/Newton algorithms based on autoregresive modeling and their application to acoustic echo cancellation. IEEE Trans. Signal Processing, 1997, 45(8)

[3] G. V. Moustakides and S. Theodoridis. Fast newton transvasal filters—A new class of adaptive estimation algorithm. IEEE Trans. Signal Processing, 1991, 39(10): 2184~2193

[4] 维德罗等著, 王永德等译. 自适应信号处理. 四川大学出版社, 1991

[5] S. Thomas Alexander. Adaptive signal processing theory and apllications, Springer-Verlag, New York Inc, 1986

[6] 王永德. 有色高斯噪声景下信号的最佳处理——自适应逆谱滤波. 四川大学学报, 1985, (4): 66~75



王永德 四川大学教授, 1962 年毕业于无线电系, 1981~1982 年美国康奈尔大学作访问学者. 现为中国电子学会信号处理学会委员, 四川大学 TI DSP 实验室主任. 主要研究方向为自适应信号处理在通信, 雷达中的应用, 全数字化高速 Modem DSP 实现.



王春霞 1975 年生, 四川大学无线电系 98 级硕士研究生. 主要研究方向为模式识别与信号处理及其 DSP 实现.

(上接第 30 页)

参考文献

[1] Evans, A., Kantrowitz, W.. A user authentication scheme for requiring secrecy in the computer. Comm. ACM, 1974, 17(8): 437~442

[2] Lennon, R. E., Matyas, S. M.. Cryptographic authentication of time-invariant quantities. IEEE Trans. Comm., 1981, 29(6): 773~777

[3] Lamport, L.. Password authentication with insecure communication. Comm. ACM, 1981, 24(11): 770~773

[4] Chang, C. C., Wu, T. C.. Remote password authentication with smart cards. IEE Proc. E, 1991, 138(3): 165~168

[5] Chang, C. C., Laih, C. S.. Correspondence for remote password authentication with smart cards. IEE Proc. E, 1992, 139(4): 372~375

[6] Chang, C. C., Hwang, S. J.. Using smart cards to authenticate remote passwords. Comput. Math. Applic., 1993, 26(7): 19~27

[7] Wu, T. C. Remote login authentication scheme based on a geometric approach. Comput. Commun., 1995, 18(12): 959~963

[8] Wu, T. C., Yeh, Y. S.. A conference key distribution system based on crossproduct. Comput. Math. Applic., 1993, 25(4): 39~46

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net