第 55 卷 第 12 期 2006 年 12 月
1000-3290/2006/55(12)/6243-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.55, No.12, December, 2006

一种多混沌系统公钥密码算法的安全性分析*

王 开† 裴文江 邹留华 何振亚

(东南大学无线电工程系,南京 210096)

(2005 年 10 月 27 日收到;2006 年 7 月 31 日收到修改稿)

最近,Ranjan 利用 m 组混沌系统及线性变换组合方法提出一种混沌公钥密码.安全分析表明攻击该公钥密码难度为 $(NP)^m$,其中 N,P 分别为密钥空间大小及线性变换复杂度.由于向量任意的线性变换都能映射为向量 2-范数简单的幅度变化,据此提出一种仅依赖公钥、初始向量及算法结构的私钥攻击算法.分析与实验结果均表明该多混沌公钥密码无法抵抗此类攻击,并且该分析方法可以有效攻击各种多混沌公钥密码算法.

关键词:公钥密码,多混沌系统,密码分析

PACC:0545

1. 引 言

由于混沌的初始值敏感性、遍历性等基本特性均与密码学中的混淆与扩散机制具有本质联系,因此近年来基于同步技术的混沌保密通信与数字化混沌(伪混沌)密码研究得到快速发展,并且在混沌序列密码、混沌分组密码方面已取得了大量研究成果[1—4].

目前,混沌公钥密码研究虽处于起步阶段,但由于已显示出若干优良密码学性质,混沌公钥密码引起了普遍关注.例如,Tenny 等[5,6]首先提出基于分布式动力学混沌公钥密码,将一个多维动力学系统分解为两个子系统,并通过交互内嵌子系统状态信息与明文信息的标量信号来实现非对称加密.文献[7,8]分别利用 Chebyshev/Jacobian 椭圆函数 Chebyshev 分数映射的半群性质设计了多种整数/实数类 Rivest-Shamir-Adleman(RSA)算法和类 ElGamal 算法,并用于密钥协商、数字签名、Hash 链、可否认认证协议设计等.研究结果表明:其中有若干方案明显不安全[9],无法抵抗基于 Chebyshev 映射共振特性的统计攻击[10];另外,此类算法也不能满足抗碰撞条件[11].Kanter 等基于混沌神经网络互学习实现了 Diffie-Hellman 框架下的渐近密钥交换协议(称为 KKK 协议)[12—15].由于同时具有教师和学生角色,互学习没有固定目标函数,因此同步后状态呈'混沌'轨道.尽管几何攻击及概率攻击等都能在较小计算量下对该协议进行破解,但由于具有交换很少信息却能协商出大量密钥的特点,因此,文献[16]认为 KKK 协议使得一种快速、低存储复杂度、基于数学之外的密钥交换协议成为可能,为通过公共信道上的协商来进行密钥交换提供了崭新的思路.在 KKK 协议的基础上,我们提出的同步和混沌分离方法可将几何攻击概率降到强力攻击水平,并在 1:3 密钥交换效率下 KKK 协议最强的组合攻击成功率仅为 2^{-128}[17].

最近,Ranjan[18]提出一类基于多混沌系统的公钥密码算法,为混沌公钥密码提供了另一种新途径.该算法首先将 Li 等[19]提出的多混沌系统伪随机数发生器推广到 m 组情况,然后在此基础上结合 m 个线性变换并在 Diffie-Hellman 协议[20]框架下设计公钥密码算法[18].安全分析表明,攻击该算法等价求解 Diffie-Hellman 难题,即只能采用强力攻击,且难度为 $(NP)^m$,其中 N,P 和 m 分别为密钥空间大小、线性变换计算复杂度和线性变换个数[18].

由于向量任意的线性变换,都能映射为向量 2-范数简单的幅度变化,本文据此提出一种仅依赖公钥、初始向量以及算法结构(显然在公钥密码中上述参数为公开参数或通过公共信道以明文形式传输)

* 国家自然科学基金(批准号:60672095)、国家高技术研究发展计划(批准号:2003AA3040)和东南大学优秀青年教师基金资助的课题.

† E-mail:kaiwang@seu.edu.cn

的私钥攻击算法.以文献[18]示例及其扩展算法为例,对该公钥密码进行安全性分析.分析及实验结果均表明该类多混沌公钥密码无法抵抗此类攻击,此外,该分析方法普遍适用于各种多混沌公钥密码算法.

2. 多混沌系统公钥密码算法安全性分析

基于多混沌系统的密钥交换算法如图 1[18] 所示,该算法分为 5 个步骤(以 $m=2$ 为例).

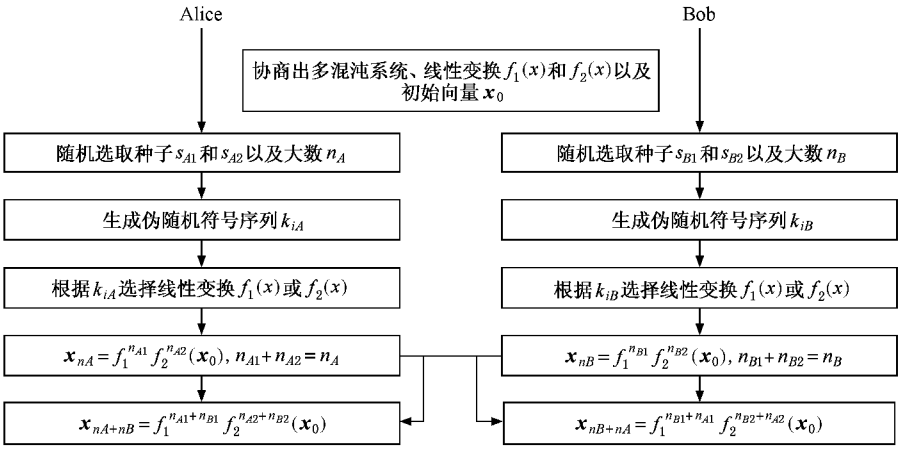

图 1 基于多混沌系统的密钥交换协议

步骤 1 通信双方 Alice 和 Bob 公开协商出线性变换 $f_1(x)$和 $f_2(x)$、混沌映射 $F_1(x)$和 $F_2(x)$以及初始向量 $\boldsymbol{x}_0$.

步骤 2 Alice 随机选取种子 s_{A1},s_{A2}以及大数 $n_A\in[0,N]$,输入到多混沌系统伪随机序列发生器中以产生 {0,1}伪随机符号序列 k_{iA},其中 n_A 为符号序列 k_{iA}的长度.根据 k_{iA}将 $\boldsymbol{x}_0$ 迭代 n_A 次产生 $\boldsymbol{x}_{nA}$,并将 $\boldsymbol{x}_{nA}$作为公钥发给 Bob,

$$x_i = h(x_{i-1},k_i), \tag{1}$$

$$h(x,k)=\begin{cases}f_1(x) & (k=0),\\ f_2(x) & (k=1).\end{cases} \tag{2}$$

步骤 3 同理,Bob 秘密选取种子 s_{B1},s_{B2}以及大数 $n_B\in[0,N]$,并输入到多混沌系统伪随机序列发生器中以产生 {0,1}随机符号序列 k_{iB},其中 k_{iB}为符号序列 k_{iB}的长度.根据 k_{iB}将 $\boldsymbol{x}_0$ 迭代 n_B 次产生 $\boldsymbol{x}_{nB}$,并将 $\boldsymbol{x}_{nB}$作为公钥发给 Alice.

步骤 4 Alice 根据 k_{iA}将 $\boldsymbol{x}_{nB}$迭代 n_A 次得到 $\boldsymbol{x}_{nB+nA}$.

步骤 5 Bob 根据 k_{iB}将 $\boldsymbol{x}_{nA}$迭代 n_B 次得到 $\boldsymbol{x}_{nA+nB}$.

由于 $f_1(x)$和 $f_2(x)$均为线性变换,且 $f_1\circ f_2=f_2\circ f_1$,因此

$$\begin{aligned}\boldsymbol{x}_{nB+nA} &= f_1^{n_{A1}}f_2^{n_{A2}}(\boldsymbol{x}_{nB})\\ &= f_1^{n_{A1}}f_2^{n_{A2}}f_1^{n_{B1}}f_1^{n_{B2}}(\boldsymbol{x}_0)\\ &= f_1^{n_{A1}+n_{B1}}f_2^{n_{A2}+n_{B2}}(\boldsymbol{x}_0),\end{aligned}$$

其中 n_{A1},n_{A2},n_{B1},n_{B2}分别为 k_{iA}与 k_{iB}中 0 和 1 的个数,显然 $n_{A1}+n_{A2}=n_A$,$n_{B1}+n_{B2}=n_B$.同理可知

$$\boldsymbol{x}_{nA+nB} = f_1^{n_{A1}+n_{B1}}f_2^{n_{A2}+n_{B2}}(\boldsymbol{x}_0).$$

因此,$\boldsymbol{x}_{nB+nA}=\boldsymbol{x}_{nA+nB}$,并作为实际使用的私钥.

该算法中由两组混沌伪随机序列发生器产生符号序列 k_i 选择不同的混沌映射 F_1 和 F_2,根据初始种子 $x_1(0)$,$x_2(0)$分别迭代 F_1 和 F_2 产生相应混沌序列 $\{x_1(k)\}$,$\{x_2(k)\}$,并根据下式求得相应的符号序列 k_i[19]:

$$k_i=\begin{cases}1 & (x_1(i)\geqslant x_2(i)),\\ 0 & (x_1(i)<x_2(i)).\end{cases} \tag{3}$$

Ranjan[18] 对此混沌公钥密码的分析显示,其攻击难度等价于求解 Diffie-Hellman 难题.如果适当选择线性变换$f(x)$,那么攻击者很难求解出由初始向量 $\boldsymbol{x}_0$ 到公钥 $\boldsymbol{x}_{nA}$,$\boldsymbol{x}_{nB}$的操作过程,求解私钥 $\boldsymbol{x}_{nA+nB}$的唯一方法只能采用强力攻击方法.假设 n_A 与 n_B 的值在 $[0,N]$ 之间随机选择,且每个线性变换 $f_1(x)$,$f_2(x)$,…,$f_m(x)$需要 P 量级次数的浮点运算,那么密钥交换双方需要进行 NP 次运算,而攻击者只能枚举所有可能情况,因此其攻击难度为 $(NP)^m$ 次运算.

3. 多混沌系统公钥密码安全性分析

n 维向量 $\boldsymbol{\eta}=(\eta_1,\eta_2,\cdots,\eta_n)^{\mathrm{T}}$ 及其线性变换 f，可以表示成

$$f(\boldsymbol{\eta})=A(\eta_1,\eta_2,\cdots,\eta_n)^{\mathrm{T}},$$

其中 A 为 $n\times n$ 维矩阵. 由于

$$f^m(\boldsymbol{\eta})=A^m(\boldsymbol{\eta}),$$

因此公钥 $\boldsymbol{x}_{nA}$ 可表示为

$$\boldsymbol{x}_{nA}=A_1^{n_{A1}}A_2^{n_{A2}}(\boldsymbol{x}_0),$$

其中矩阵 A_1,A_2 分别表示为线性可逆变换 $f_1(x)$ 及 $f_2(x)$ 的满秩变换矩阵. 由于 $f_1\circ f_2=f_2\circ f_1$，因此矩阵 A_1,A_2 必须可交换，即 $A_1A_2=A_2A_1$.

文献[18]中的安全分析表明，如果适当选择线性变换 $f(x)$，那么攻击者很难求解出由初始向量 $\boldsymbol{x}_0$ 到公钥 $\boldsymbol{x}_{nA}$ 及 $\boldsymbol{x}_{nB}$ 的操作过程，即攻击者很难攻击出 $f_1(x)$ 及 $f_2(x)$ 的实际迭代次数 n_{A1},n_{A2} 以及 n_{B1},n_{B2}. 可是任意向量可逆线性变化前后，其 2-范数间存在如下对应关系：已知 n 维向量 $\boldsymbol{x}$ 以及一个 $n\times n$ 的满秩矩阵 A. 令 n 维向量 $\boldsymbol{y}_m=A^m\boldsymbol{x}$ 且 b_m 为向量 $\boldsymbol{y}_m$ 的 2-范数，则存在 $\lim\limits_{m\to\infty}(b_{m+1}/b_m)=\lambda_{\max}$，其中 $\lambda_{\max}$ 为矩阵 A 的最大特征值.

证明　令 V,D 分别表示矩阵 A 的特征向量阵和特征值对角阵，则 $A=V^{-1}DV$，因此

$$\boldsymbol{y}_m=A^m\boldsymbol{x}=(V^{-1}DV)^m\boldsymbol{x}=V^{-1}D^mV\boldsymbol{x},$$

$$\boldsymbol{y}_{m+1}=V^{-1}D^{m+1}V\boldsymbol{x}.$$

再令 $D=\mathrm{diag}[\lambda_1,\lambda_2,\cdots,\lambda_n]$，$V^{-1}=\{a_{ij}\}_{n\times n}$，$V\boldsymbol{x}=(x_1,x_2,\cdots,x_n)'$，分别计算 $\boldsymbol{y}_m$ 和 $\boldsymbol{y}_{m+1}$ 2-范数可得

$$b_m=\|\boldsymbol{y}_m\|_2=\sqrt{\sum_{i=1}^{n}\Big(\sum_{j=1}^{n}a_{ij}\lambda_j^m x_j\Big)^2},$$

$$b_{m+1}=\|\boldsymbol{y}_{m+1}\|_2=\sqrt{\sum_{i=1}^{n}\Big(\sum_{j=1}^{n}a_{ij}\lambda_j^{m+1} x_j\Big)^2}.$$

当 m 取值趋于无穷时，求极限

$$\lim_{m\to\infty}(b_{m+1}/b_m)^2=\frac{\sum\limits_{i=1}^{n}\Big(\sum\limits_{j=1}^{n}a_{ij}\lambda_j^{m+1}x_j\Big)^2}{\sum\limits_{i=1}^{n}\Big(\sum\limits_{j=1}^{n}a_{ij}\lambda_j^{m}x_j\Big)^2}=\frac{\lambda_{\max}^{2m+2}\sum\limits_{i=1}^{n}\Big(\sum\limits_{j=1}^{n}a_{ij}\lambda_j\Big(\frac{\lambda_j}{\lambda_{\max}}\Big)^m x_j\Big)^2}{\lambda_{\max}^{2m}\sum\limits_{i=1}^{n}\Big(\sum\limits_{j=1}^{n}a_{ij}\Big(\frac{\lambda_j}{\lambda_{\max}}\Big)^m x_j\Big)^2}. \tag{4}$$

当 $\lambda_j\neq\lambda_{\max}$ 时，$\lim\limits_{m\to\infty}(\lambda_j/\lambda_{\max})^m=0$，因此

$$\lim_{m\to\infty}(b_{m+1}/b_m)=\lambda_{\max}.$$

证毕.

向量间任意复杂的线性变换，对应其 2-范数，仅是简单的幅度变化. 分别计算公钥 $\boldsymbol{x}_{nA}$ 和初始向量 $\boldsymbol{x}_{nA}$ 的 2-范数，则有如下近似式成立：

$$\|\boldsymbol{x}_{nA}\|_2\approx\lambda_{A1}^{n_{A1}}\lambda_{A2}^{n_{A2}}\|\boldsymbol{x}_0\|_2, \tag{5}$$

其中 $\lambda_{A1},\lambda_{A2}$ 分别表示满秩矩阵 A_1,A_2 的最大特征值.

根据(5)式可知，范数 $\|\boldsymbol{x}_{nA}\|_2$ 随着 n_{A1},n_{A2} 的增长而呈指数增长，因此多混沌系统公钥密码算法必然存在密钥空间小的缺点. 若计算机的计算精度为 2^{51}，那么当 $n_{A1}>|\log_{\lambda_{A1}}2^{51}|$ 时，$\lambda_{A1}^{n_{A1}}$ 将溢出，此时密钥空间 N 仅为 $\min\{|\log_{\lambda_{A1}}2^{51}|,|\log_{\lambda_{A2}}2^{51}|\}$.

加密算法的安全性应仅依赖于密钥信息，根据(5)式给出一种泛化的攻击方法. 仅依据公开协商的初始向量 $\boldsymbol{x}_0$ 和公钥 $\boldsymbol{x}_{nA}$ 即可以求出 n_{A1},n_{A2}. 进一步根据公钥 $\boldsymbol{x}_{nB}$，可容易攻击出私钥 $\boldsymbol{x}_{nA+nB}$.

步骤 1　求初始向量 $\boldsymbol{x}_0$ 的 2-范数，线性可逆变换 $f_1(x),f_2(x)$ 的满秩变换矩阵 A_1,A_2 的最大特征值 $\lambda_{A1},\lambda_{A2}$.

步骤 2　求公钥 $\boldsymbol{x}_{nA}$ 的 2-范数. 结合步骤 1 的结果，可得 $S=\|\boldsymbol{x}_{nA}\|_2/\|\boldsymbol{x}_0\|_2$，显然 $S\approx\lambda_{A1}^{n_{A1}}\lambda_{A2}^{n_{A2}}$.

步骤 3　定义变量 I_{n1} 及 I_{n2}，并将 I_{n2} 从零开始枚举 $C=S/(\lambda_{A2})^{I_{n2}}$，求相应的 $I_{n1}=\mathrm{round}(\log_{\lambda_{A1}}C)$，其中 $\mathrm{round}(\cdot)$ 为四舍五入函数. 计算 $f_1^{I_{n1}}f_2^{I_{n2}}(\boldsymbol{x}_0)$.

步骤 4　重复步骤 3，直至 $\boldsymbol{x}_{nA}=f_1^{I_{n1}}f_2^{I_{n2}}(\boldsymbol{x}_0)$. 此时 I_{n1} 和 I_{n2} 分别为 n_{A1} 和 n_{A2}.

步骤 5　将公钥 $\boldsymbol{x}_{nB}$ 分别进行 n_{A1} 次 $f_1(x)$ 操作，n_{A2} 次 $f_2(x)$ 操作，可得最终私钥 $\boldsymbol{x}_{nA+nB}$.

4. 实验结果及分析

由于任意向量线性变换前后的 2-范数都存在简单的幅度变化关系，据此提出的上述泛化攻击方法普遍适用于任意多混沌公钥算法，而不再仅仅适用于某个具体的算法实例. 以文献[18]示例及扩展算法为例，下面将证明这种泛化攻击方法的有效性以及普遍适用性.

以文献[18]中的范例为例，初始向量 $\boldsymbol{x}_0$、线性变换 $f_1(x),f_2(x)$ 以及混沌映射 $F_1(x),F_2(x)$ 分

别为

$$\begin{aligned} \boldsymbol{x}_0 &= [0.06,0.35,0.81,0.01,0.14],\\ f_1(x) &= \mathrm{FFT}(x),\\ f_2(x) &= 1.5x,\\ F_1(x_n) &= 4x_n(1-x_n),\\ F_2(x_n) &= 3.98x_n(1-x_n). \end{aligned}$$

这里 FFT(·)表示快速傅里叶变换. Alice 随机选取的种子为 {0.83,0.34},并且 $n_A=10$;Bob 选取的种子为 {0.47,0.61},并且 $n_B=12$,则产生的 k_A,k_B 分别为[1,0,1,0,1,10,1,0,1],[0,1,0,0,0,1,1,0,0,1,1,1]. 依据密钥交换步骤可知,$\boldsymbol{x}_{nA}$,$\boldsymbol{x}_{nB}$ 分别为[37.9,88.59,6.33,512.58,221.48],[8.5,199.3,14.2,1153.3,498.3],最终协商出的私钥 $\boldsymbol{x}_{nA+nB}$ 为[5410,315360,729820,9010,126140].

对于 M 维向量 $\boldsymbol{x}$,记 $\boldsymbol{X}=\mathrm{FFT}(\boldsymbol{x})$,则存在等式

$$M\sum_{n=0}^{M-1}|\boldsymbol{x}(n)|^2=\sum_{k=0}^{M-1}|\boldsymbol{X}(k)|^2,$$

(5)式可改写为

$$\|\boldsymbol{x}_{nA}\|_2^2=M^{n_{A1}}(1.5)^{2n_{A2}}\|\boldsymbol{x}_0\|_2^2. \tag{6}$$

泛化的攻击步骤可以简化如下:

步骤 1 根据初始向量 $\boldsymbol{x}_0$,可得 $\|\boldsymbol{x}_0\|_2^2=0.7983$.

步骤 2 根据公钥 $\boldsymbol{x}_{nA}$,可得 $\|\boldsymbol{x}_{nA}\|_2^2=319695$. 结合步骤 1 的结果,可得 $S=M^{n_{A1}}(1.5)^{2n_{A2}}=4.0045\times10^5$.

步骤 3 将 I_{n2} 从零开始枚举直至正整数 $I_{n1}=\log_M C$,其中 $C=S/(1.5)^{2I_{n2}}$. 易知此时 I_{n1} 和 I_{n2} 分别为 n_{A1} 和 n_{A2}. 在上例中,当枚举至 $I_{n2}=4$ 时,使得 $C=15625$,亦即 I_{n1} 取值为 6.

步骤 4 将公钥 $\boldsymbol{x}_{nB}$ 分别进行 n_{A1} 次 $f_1(x)$ 操作,n_{A2} 次 $f_2(x)$ 操作,可得到最终私钥 $\boldsymbol{x}_{nA+nB}$ 为[5410,315360,729820,9010,126140].

泛化攻击方法不仅适用于快速傅里叶变换,还适用于其他各种线性变换. 仍以文献[18]中的范例为例,将线性变换 $f_2(x)$ 替换为离散余弦变换(DCT):$f_2(x)=\mathrm{DCT}(x)$,其余初始条件不变. 计算可知 $\boldsymbol{x}_{nA}$,$\boldsymbol{x}_{nB}$ 分别为

$$\begin{aligned} \boldsymbol{x}_{nA} &= [-0.99,62.45,26.87,87.54,-15.59],\\ \boldsymbol{x}_{nB} &= [-11.69,73.17,35.20,62.74,-43.18]. \end{aligned}$$

最终协商出的私钥 $\boldsymbol{x}_{nA+nB}$ 为[7954,-1549,5214,-8984,4713].

对于 M 维向量 $\boldsymbol{x}$,若记 $\boldsymbol{X}=\mathrm{DCT}(\boldsymbol{x})$,则存在等式

$$\sum_{n=0}^{M-1}|\boldsymbol{x}(n)|^2=\sum_{k=0}^{M-1}|\boldsymbol{X}(k)|^2,$$

(5)式可改写为

$$\|\boldsymbol{x}_{nA}\|_2^2=M^{n_{A1}}\|\boldsymbol{x}_0\|_2^2. \tag{7}$$

泛化的攻击步骤可以简化如下:

步骤 1 根据初始向量 $\boldsymbol{x}_0$,公钥 $\boldsymbol{x}_{nA}$,可得 $S=M^{n_{A1}}=15625$,从而解得 $n_{A1}=6$.

步骤 2 将 I_{n2} 从 1 开始枚举直至 $I_{n2}=4$,使 $\mathrm{FTT}^{n_{A1}}(\mathrm{DCT}^{I_{n2}}(\boldsymbol{x}_0))=\boldsymbol{x}_{nA}$. 此时 I_{n2} 即为 n_{A2}.

步骤 3 将公钥 $\boldsymbol{x}_{nB}$ 分别进行 n_{A1} 次 $f_1(x)$ 操作,n_{A2} 次 $f_2(x)$ 操作,可得到最终私钥 $\boldsymbol{x}_{nA+nB}$ 为[7954,-1549,5214,-8984,4713].

5. 结 论

由于任意向量复杂的线性变化,对应其 2-范数仅是简单的幅度变化. 本文据此对一类基于多混沌系统的公钥协商算法进行了安全性分析,通过比较线性变换前后向量的 2-范数,获得初始向量 $\boldsymbol{x}_0$ 和公钥 $\boldsymbol{x}_{nA}$ 及 $\boldsymbol{x}_{nB}$ 间的对应关系,并进一步得到私钥 $\boldsymbol{x}_{nA+nB}$. 分析与实验结果均表明,该多混沌公钥密码无法抵抗此类攻击. 该分析方法可以有效攻击各种多混沌公钥密码算法.

[1] Jakimoski G, Kocarev L 2001 *IEEE Trans. Circ. Syst.* Ⅰ **48** 163

[2] Baptista M S 1998 *Phys. Lett.* A **240** 50

[3] Lü H P, Wang S H, Li X W *et al* 2004 *Chin. Phys.* **13** 626

[4] Li J F, Li N 2002 *Chin. Phys.* **11** 1124

[5] Tenny R, Tsimring L S, Larson L *et al* 2003 *Phys. Rev. Lett.* **90** 047903

[6] Tenny R, Tsimring L S 2005 *IEEE Trans. Circ. Syst.* Ⅰ **52** 672

[7] Kocarev L, Sterjev M, Fekete A *et al* 2004 *Chaos* **14** 1078

[8] Xiao D, Liao X F, Wong K 2005 *Chaos Solitons Fract.* **23** 1327

[9] Alvarez G 2005 *Chaos Solitons Fract.* **26** 7

[10] Kohda T, Yosimura T 2004 *Proc. ISCAS* **4** 573

[11] Bergamo P, D'Arco P, Santis A *et al* 2005 *IEEE Trans. Circ. Syst.* Ⅰ **25** 1382

[12] Kanter I, Kinzel W, Kanter E 2002 *Europhys. Lett.* **57** 141

[13] Mislovaty R, Klein E, Kanter I *et al* 2003 *Phys. Rev. Lett.* **91** 118701
[14] Ruttor A, Kinzel W, Shacham L *et al* 2004 *Phys. Rev.* E **69** 046110
[15] Klein E, Mislovaty R, Kanter I *et al* 2005 *Phys. Rev.* E **72** 016214
[16] Kilmov A, Mityagin A, Shamir A 2002 *Lecture Note Comput. Sci.* **2501** 288
[17] Zhou J T, Xu Q Z, Pei W J *et al* 2004 *Int. J. Neur. Sys.* **14** 393
[18] Ranjan B 2005 *Phys. Rev. Lett.* **95** 098702
[19] Li S J, Mou X Q, Cai Y L 2001 *Proc. INDOCRYPT* **2247** 316
[20] Diffie W, Hellman M E 1976 *IEEE Trans. Inform. Theory* **22** 454

Cryptanalysis of multiple chaotic systems based public key encryption technique*

Wang Kai† Pei Wen-Jiang Zou Liu-Hua He Zhen-Ya
(*Department of Radio Engineering, Southeast University, Nanjing* 210096, *China*)
(Received 27 October 2005; revised manuscript received 31 July 2006)

Abstract

A novel public key encryption technique based on multiple chaotic systems has been proposed. This scheme employs m-chaotic systems and a set of linear functions for key exchange over an insecure channel. The security of the proposed algorithm grows as $(NP)^m$, where N, P are the size of the key and the computational complexity of the linear functions, respectively. In this paper, the fundamental weakness of the cryptosystem is pointed out and a successful attack is described. Given the fact that any complex linear transformations on a vector will make the norm of the vector approximate linear growth, we present an attack that permits recovering the corresponding secret key from the public key and the initial value. Both theoretical and experimental results show that the attacker can access the secret key without any difficulty. The lack of security discourages the use of such algorithm for practical applications.

Keywords: public key cryptography, multiple chaotic systems, cryptanalysis
PACC: 0545

* Project supported by the National Natural Science Foundation of China (Grant No. 60672095), the National High Technology Development Program of China (Grant No. 2003AA3040) and the Foundation for Excellent Young Teachers of Southeast University, China.

† E-mail: kaiwang@seu.edu.cn