一类时空混沌加解密系统的安全分析*

王 开† 裴文江 周建涛 张毅峰 周思源

(东南大学无线电工程系,东南大学水声信号处理教育部重点实验室,南京 210096)

(2010 年 8 月 24 日收到;2010 年 10 月 8 日收到修改稿)

本文安全分析文献[*Phys. Rev.* E **66** 065202 (2002)]所提的一类自同步的时空混沌流密码系统. 发现该高维的加解密系统在常数的驱动下将收敛到一维,使得动力学系统的复杂性大为降低. 在某些特定输入区域内容,保密系统对输入状态的微小扰动不敏感. 可以建立密钥和特殊输入状态间一个简单的线性关系,并依次从密钥流中恢复出密钥. 基于此,提出一套选择密文攻击方法,利用系统参数和扰动前后密钥流的差异之间的依赖关系通过寻优算法破解密钥,从而攻击了上述文献所提出的基于混沌自同步的安全通信算法.

关键词: 混沌密码, 耦合映像格子, 安全分析

PACS: 05.45.-a, 05.45.Ra, 05.45.Vx

1. 引 言

在有限精度情况下,任意数字化混沌都会导致动其力学退化,从而使得原混沌轨道退化为周期轨道. 而通过耦合,耦合混沌系统能够产生适用于实际安全传输要求的长周期轨道. 由于耦合系统具有大量的正 Lyapunov 指数,因此由耦合系统产生的时空轨道具有复杂的类随机特性. 由于耦合系统中所具有的多节点结构,因此可以同时产生多路相互独立的密钥流,从而提高了加密效率. 由于耦合混沌系统具有一维混沌所不具有的密码学特性,因此研究者在设计基于耦合混沌系统的序列密码方面开展了大量工作.

目前,基于耦合映像格子的混沌密码算法共有两类设计思想,其中之一是基于符号化手段,以耦合系统的控制参数和初始条件为密钥,通过符号化系统的动力学轨迹而得到多径伪随机符号序列,并依次设计相应的混沌密码算法[1—4]. 随着符号向量动力学的提出,由于攻击者可以通过观测到的符号向量学重构出密钥,因此这类算法大多存在安全缺陷[5,6];而另一类设计思想则是基于混沌同步技术设计混沌保密通信算法. 自 Pecora 与 Carroll 提出混沌同步方法以来[7],混沌保密通信技术得到广泛研究. 文献[8]将单向耦合映像格子和一些基本的代数操作的结合,构造出自同步的时空混沌流密码系统. 通过级联的方式,可以有效提高同步对系统参数的不敏感性. 研究表明密码系统对控制参数的敏感性随着耦合级数的增加而指数上升. 通过引入渐进确定性随机或在耦合结构的中间格点嵌入 S 盒操作可以使得系统在附加计算量很小的情况下进一步提高密钥敏感[9—12]. 文献[13]将耦合结构扩展至二维,使得从不同格点产生的密钥流可以进行并行的加解密,从而极大地提高加解密的速度. 在上述密码系统基础上,还分别衍生出混沌公钥密码和 Hash 算法[11,14]. 分析和实验结果表明这类系统的周期在双精度和系统耦合规模为 20 的条件下超过 10^{140}. 目前攻击算法对它进行的安全性分析表明原型算法能抵抗所有攻击. 其中,基于统计特性的攻击算法不成功的原因在于所产生的密钥流具有非常好的统计学特性. 从获得的密文很难获得明文的一些信息.

另一方面,尽管安全分析表明这类基于混沌同步的保密通信系统具有最优的整体密码学特性,包

* 国家自然科学基金(批准号: 60672095, 60972165), 国家高技术研究发展计划(863 计划)(批准号: 2007AA11Z210), 教育部博士点基金(批准号: 20100092120012,20070286004), 江苏省高技术研究项目,江苏省自然科学基金(批准号:BK2010240), 国家十一五密码发展基金,国家火炬计划项目资助的课题.

† E-mail: kaiwang@seu.edu.cn

括安全性、同步的快速性和优良的抗噪声性能,比单独应用混沌和经典密码加解密的性能都好,甚至优于目前流行的 AES (advanced encryption standard),但同样存在安全缺陷. 文献[15]认为文献[8]所提出密码系统存在两点安全缺陷:1)密文的产生同其信息长度无关;2)算法中的模操作存在安全缺陷,并据此提出了相应的攻击方法. 通过一组明文/密文对,攻击者可以得到其余 $2^v - 1$ 个相应的明文/密文对.

本文我们将安全分析文献[8]中所提出的原型自同步的时空混沌流密码系统. 我们发现该高维的加解密系统在常数的驱动下将收敛到一维,使得动力学系统的复杂性大为降低. 在某些特定输入区域内容,保密系统对输入状态的微小扰动不敏感. 而我们可以建立密钥和特殊输入状态间一个简单的线性关系,并依次从密钥流中恢复出密钥. 基于此,我们提出一套攻击方法,利用系统参数和扰动前后密钥流的差异之间的依赖关系通过寻优算法破解密钥,从而攻击了文献[8]所提出了基于混沌自同步的安全通信算法.

2. 自同步的时空混沌流密码系统

文献[8]所提出的自同步的时空混沌流密码系统以 OCML 为基本的运算单元,通过耦合多个低维系统而有效的增加系统维数. 显然系统的安全性并不能完全依赖于系统的高维和动力学行为的复杂性,比如参数估计和误差函数攻击等方法均能有效地破解这些系统. 为此,文献[8]将取整和取模操作与 OCML 系统相结合,大大地提高了系统的安全性. 其加密机和解密机的状态方程如下所示.

发射机:

$$x_{n+1}(j) = (1-\varepsilon)f_j[x_n(j)] + \varepsilon f_j[x_n(j-1)],$$
$$f_j(x) = (3.75 + a_j/4)x(1-x),$$
$$j = 1,2,\cdots,m, \tag{1a}$$
$$x_{n+1}(j) = (1-\varepsilon)f[x_n(j)] + \varepsilon f[x_n(j-1)],$$
$$f(x) = 4x(1-x),\ j = m+1,\cdots,N \tag{1b}$$
$$S_n = (K_n + I_n)\bmod 2^v, \tag{1c}$$
$$K_n = \mathrm{int}(x_n(N)\times 2^\mu)\bmod 2^\nu, \tag{1d}$$
$$x_n(0) = S_n/2^v. \tag{1e}$$

接收机:

$$y_{n+1}(j) = (1-\varepsilon)f_j[y_n(j)] + \varepsilon f_j[y_n(j-1)],$$
$$f_j(x) = (3.75 + b_j/4)x(1-x),$$
$$j = 1,2,\cdots,m, \tag{2a}$$
$$y_{n+1}(j) = (1-\varepsilon)f[y_n(j)] + \varepsilon f[y_n(j-1)],$$
$$f(x) = 4x(1-x),\ j = m+1,\cdots,N \tag{2b}$$
$$K'_n = \mathrm{int}(y_n(N)\times 2^\mu)\bmod 2^\nu \tag{2c}$$
$$I'_n = (S_n - K'_n)\bmod 2^\nu \tag{2d}$$
$$y_n(0) = S_n/2^v = x_n(0). \tag{2e}$$

其中 I_n, K_n, S_n 和 K'_n 分别代表明文,加密密钥流,密文以及解密密钥流. 控制参数 $\boldsymbol{a} = (a_1,a_2,\cdots,a_m)$ 和 $\boldsymbol{b} = (b_1,b_2,\cdots,b_m)$ 分别作为加解密的密钥,可以在 (0,1) 中任取. 其他诸如耦合强度,耦合大小对攻击者是公开的,通常设为 $\varepsilon = 0.99$, $\mu = 52$, $\nu = 32$, $m = 4$, $N = 25$. 发射机将密文 S_n 发射到公共信道,解密机以 $y_n(0) = x_n(0) = S_n/2^\nu$ 作为驱动量,并将解密密钥和加密密钥设为一致即可与发射机同步,从而 $y_n(N) = x_n(N)$, $K'_n = K_n$, $I'_n = I_n$.

由于取模操作隐藏了密码系统的状态变量 $x_n(N)$, 因此根据密钥流 K_n 需要 $2^{\mu-\nu}$ 的计算量才能推出最后一个格点的状态变量 $x_n(N)$. 对于参数估计方法,很难构造出收敛的代价函数. 而对于逆运算代数攻击, $2^{\mu-\nu}$ 的计算量大大提高了代数求解密钥的难度. 目前已知的选择密文攻击算法求解一个密钥的算量将达 2^{20}.

3. 安全漏洞分析以及选择密文攻击

本文我们意图说明自同步的时空混沌流密码系统所存在的本质安全缺陷,为简化分析的繁琐程度,在加密端和解密端,我们仅以第一个状态方程第一项的 a_1 和 b_1 作为密钥,其余各控制参数 $(a_2\cdots a_m)$ 和 $(b_2\cdots b_m)$ 都公开且假定为 1. 此外,我们将驱动项记为 $y_d = 4y_n(0)(1-y_n(0))$.

文献[16]发现当以常数 C 作为驱动时,解密机的所有状态变量均收敛于某个不动点,且这个不动点与常量驱动有关. 实际上,对于结合了 OCML 和取整、取模运算的系统而言这个结论仍然成立. 由第一个格点的状态方程可知

$$\begin{aligned}&|y_{n+1}(1) - y_n(1)|\\ &= (1-\varepsilon)\,|f_1[y_n(1)] - f_1[y_{n-1}(1)]|\\ &< 4(1-\varepsilon)\,|y_n(1) - y_{n-1}(1)|.\end{aligned} \tag{3}$$

由于 $0 < 4(1-\varepsilon) < 1$, 有 $\lim\limits_{n\to\infty}|y_{n+1}(1) - y_n(1)| = 0$, 即第一个格点的状态将快速收敛. 重复上述类似的计算,可得 $\lim\limits_{n\to\infty}|y_{n+1}(i) - y_n(i)| = 0$, i

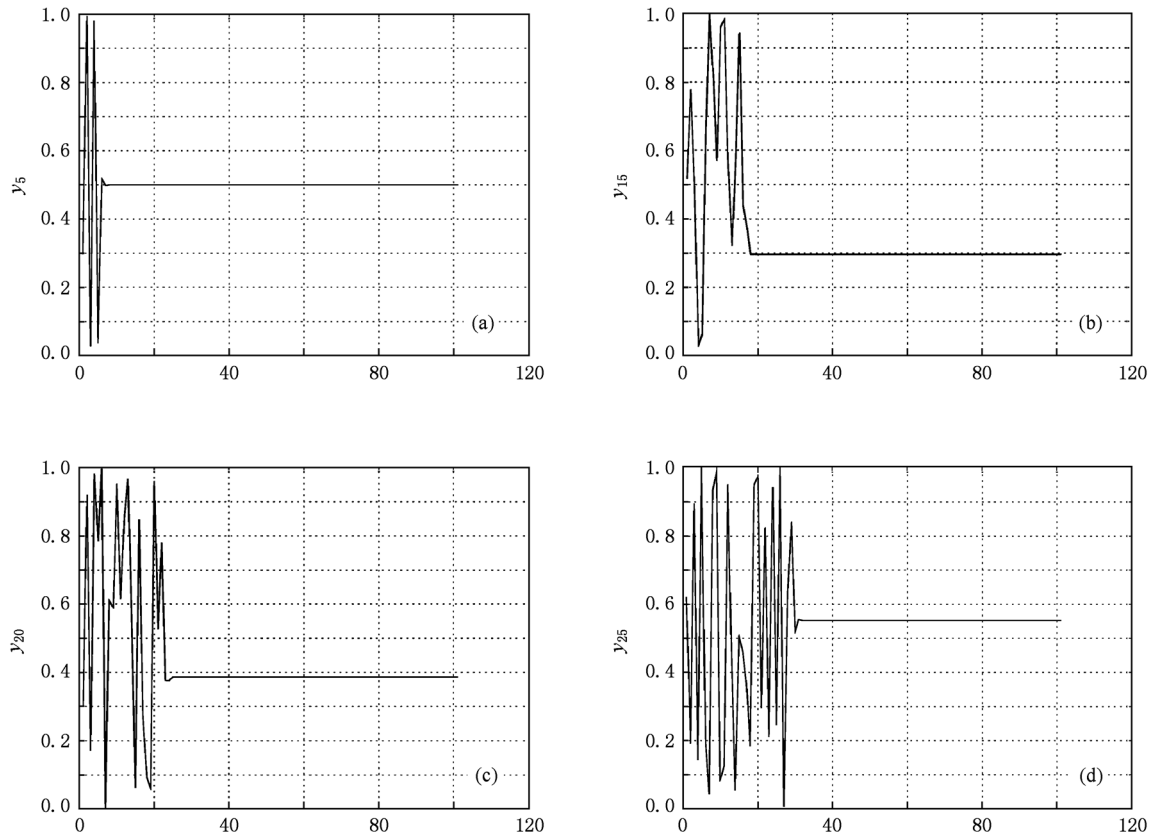

图 1 在常数 $y_d = 1/3$ 驱动下状态变量收敛情况

$= 2,3,\cdots,N$. 因此如图 1 所示,当驱动信号为常数时系统的所有格点均收敛到不动点.

在常数的驱动下,原高维系统收敛为一个一维的系统,使得对叠加于常数驱动上的扰动不敏感. 由于收敛以后每个格点的状态与时间无关,从(2)式中可以直接解出各个格点收敛的状态.

$$y_1 = \frac{R' + \sqrt{R'^2 + 4\varepsilon(R'+1)y_d}}{2(R'+1)} = \varphi(y_d),$$

$$R' = (3.75 + b_1/4)(1-\varepsilon) - 1, \tag{4a}$$

$$y_j = \frac{R + \sqrt{R^2 + 16\varepsilon(R+1)y_{j-1}(1-y_{j-1})}}{2(R+1)} = \phi(y_{j-1}),$$

$$R = 4(1-\varepsilon) - 1. \tag{4b}$$

由此可知, $y_i = \phi^{i-1}[\varphi(y_d)]$, $i = 1,2,\cdots,N$. 虽然函数 $y_i = \phi^{i-1}[\varphi(y_d)]$ 很复杂,但仍是一维的. 图2 为不同驱动量所对应收敛后的格点状态,我们发现当驱动量取在 0.495 附近时, $y_i = \phi^{i-1}[\varphi(y_d)]$ 是一个慢变的函数,意味着当驱动选择在这些区间时系统更容易控制.

自同步的时空混沌流密码系统具有高安全性. 其原因在于通过模操作,已知密钥 K_N 需要 $2^{\mu-\nu} = 2^{20}$ 次计算量才能获得最后一个格点的状态. 然而,考虑(2c)式,若两个变量 $y_n(N)$ 和 $y'_n(N)$ 满足 $|y'_n(N) - y_n(N)| < 2^{-20}$,那么它们之间的差值可由相应的密钥流 K'_n 和 K''_n 唯一确定. 因此如(5)式所示, y_N 和 K_N 在 2^{-20} 的区间内存在线性的关系,

$$y'_n(N) - y_n(N) = (K'' - K')/2^{\mu}. \tag{5}$$

假定输入常数,记 $K_1 = \mathrm{int}(y_N \times 2^{\mu}) \bmod 2^{\nu}$ 为相应的收敛的密钥流. 假定输入常数 $y'_d = y_d + \tau$, 其中 $\tau \ll 1$ 为驱动 y_d 上叠加一个微小的扰动(一般选择 $\tau = 2^{-36}$),记 $K_2 = \mathrm{int}(y'_N \times 2^{\mu}) \bmod 2^{\nu}$ 为相应的收敛的密钥流. 我们定义函数 $g(b, y_d) = K_2 - K_1$, 它描述了系统参数和扰动前后密钥流之间差异的关系.

由于系统在常数驱动下收敛后对叠加与驱动上的微小扰动不敏感,因而对于任意的密钥 $b_1 \in [0,1]$ 都存在着某个 y_{d1} 使得 $g(b_1, y_{d1}) = 0$. 即在扰动前后密钥流不发生变化. 我们称由满足 $g(b_1, y_{d1}) = 0$ 的点 (b_1, y_{d1}) 组成的区域为静止区(silent position). 扰动后的系统状态方程如(6)式所示,注

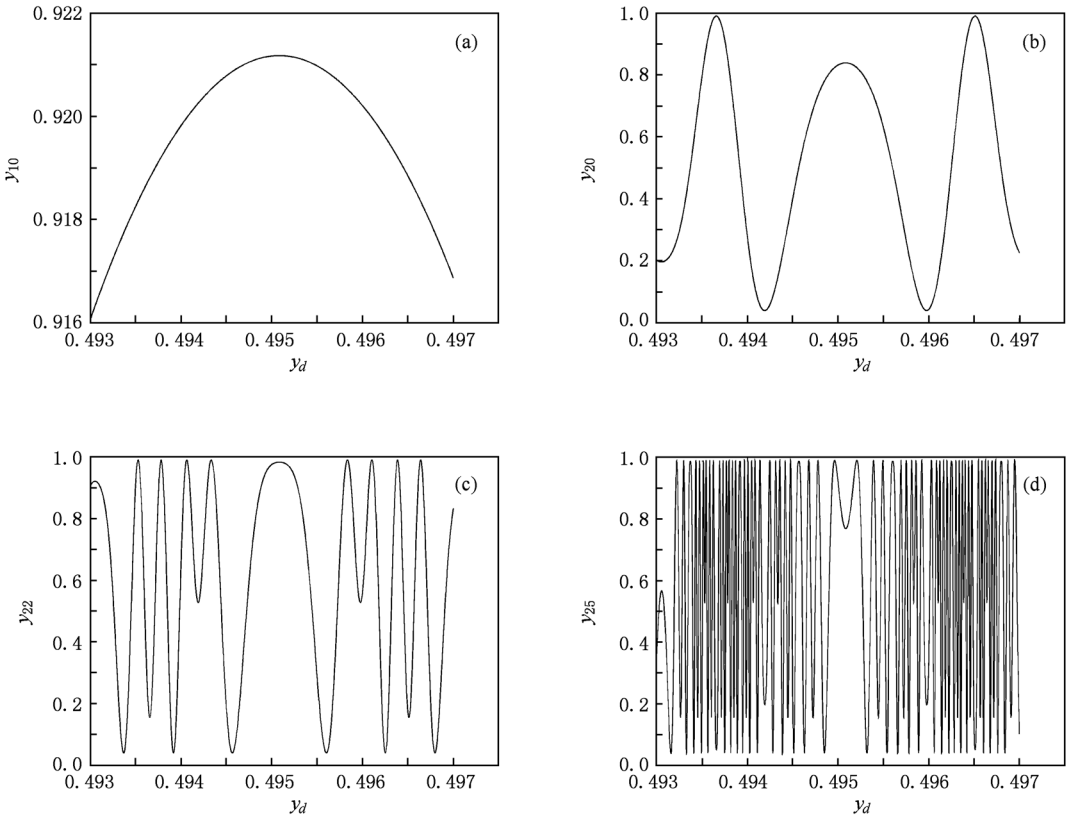

图 2 不同驱动量所对应收敛后的格点状态

意方程中右边的第一项保持不变,因为扰动对他们的影响将从下一时刻起作用.

$$y_1' = (1-\varepsilon)(3.75 + b_1/4)y_1(1-y_1) + \varepsilon(y_{d1} + \tau), \tag{6a}$$

$$y_j' = 4(1-\varepsilon)y_j(1-y_j) + 4\varepsilon y_{j-1}'(1-y_{j-1}'), \quad j = 2,3,\cdots,N. \tag{6b}$$

设定义误差函数 $e_k = y_k' - y_k$, 我们可得系统的误差动力学方程

$$e_1 = \varepsilon\tau,\ e_j = 4\varepsilon e_{j-1}(1-2y_{j-1}) - 4\varepsilon(e_{j-1})^2,\quad j = 2,3,\cdots,N. \tag{7}$$

由于 $\tau \ll 1$, $(e_{j-1})^2 \to 0$, 故(7)式可以记为

$$e_j = 4\varepsilon e_{j-1}(1-2y_{j-1}), j = 2,3,\cdots,N, \tag{8}$$

可得

$$e_j = \varepsilon\tau(4\varepsilon)^{j-1}\prod_{i=1}^{j-1}(1-2y_i),\quad j = 2,3,\cdots,N. \tag{9}$$

显然当 $y_j = 0.5, j = 1,2,\cdots,N-1$ 时,有 $g(b_1, y_{d1}) = 0$. 假设 $y_1 = 0.5$, 由(2)式可得 $y_{d1} = [2 - (1-\varepsilon)(3.75 + b_1/4)]/4\varepsilon$. 故当 $b_1 \in [0,1]$ 时,y_{d1} 的变化范围为 $\Phi = [0.49494949495, 0.49558080808]$. 值得注意的是这个区间在 0.495 周围,这也就是我们在图 2 中选择这个范围的原因. 因此,对于任意的 $b_1 \in [0,1]$, 在 Φ 中至少能找到一个 y_{d1} 使得 $g(b_1, y_{d1}) = 0$. 图 3 示出了 $|g(b,y_d)|/2^{\mu}$ 与 $b_1 \in [0,1]$ 和 $y_d \in \Phi$ 的三维图,图的底部与 $z = 0$ 平面的相交部位为静止区, 显然对于任意 $b_1 \in [0,1]$ 至少存在着一个 y_{d1} 使得 $g(b_1, y_{d1}) = 0$.

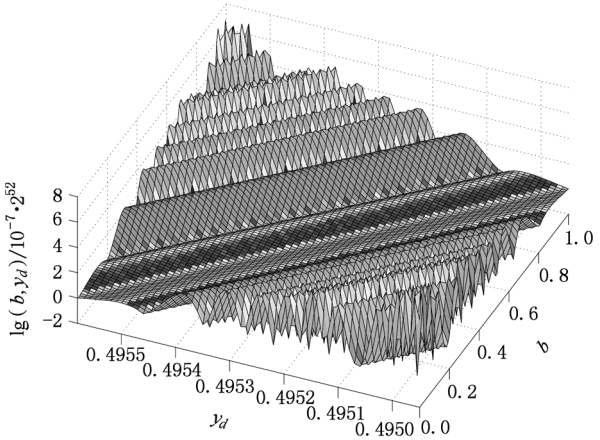

图 3 $|g(b,y_d)|/2^{\mu}$ 与 $b_1 \in [0,1]$ 的对应关系, $y_d \in \Phi$

正如图2所示,函数 $\phi^{N-1}[\varphi(x)]$ 在区间 Φ 上缓变,因此可以通过一个简单的迭代算法来寻找对应于某个密钥 b_1 的 y_{d1} 使得 $g(b_1, y_{d1}) = 0$, 如下式所示:

$$y_{d1}(k+1) = y_{d1}(k) + \gamma(K_2 - K_1)/2^v. \quad (10)$$

随机产生4组密钥 0.7865302612, 0.2167895352, 0.9622608529 和 0.5142749875, 根据用(10)式来寻找其相应的常数驱动 y_{d1}, 过程如图4所示. 实验结果显示,通过大约100步迭代即可成功找到对应的常数驱动, 分别为 0.4952069639873661, 0.4953212443515219, 0.4950960229637708 以及 0.4953788423065933 48. 每组数据均为重复计算100次的所得的平均值.

需要注意的是:若存在着一个点 (b_1, y_{d1}) 使得

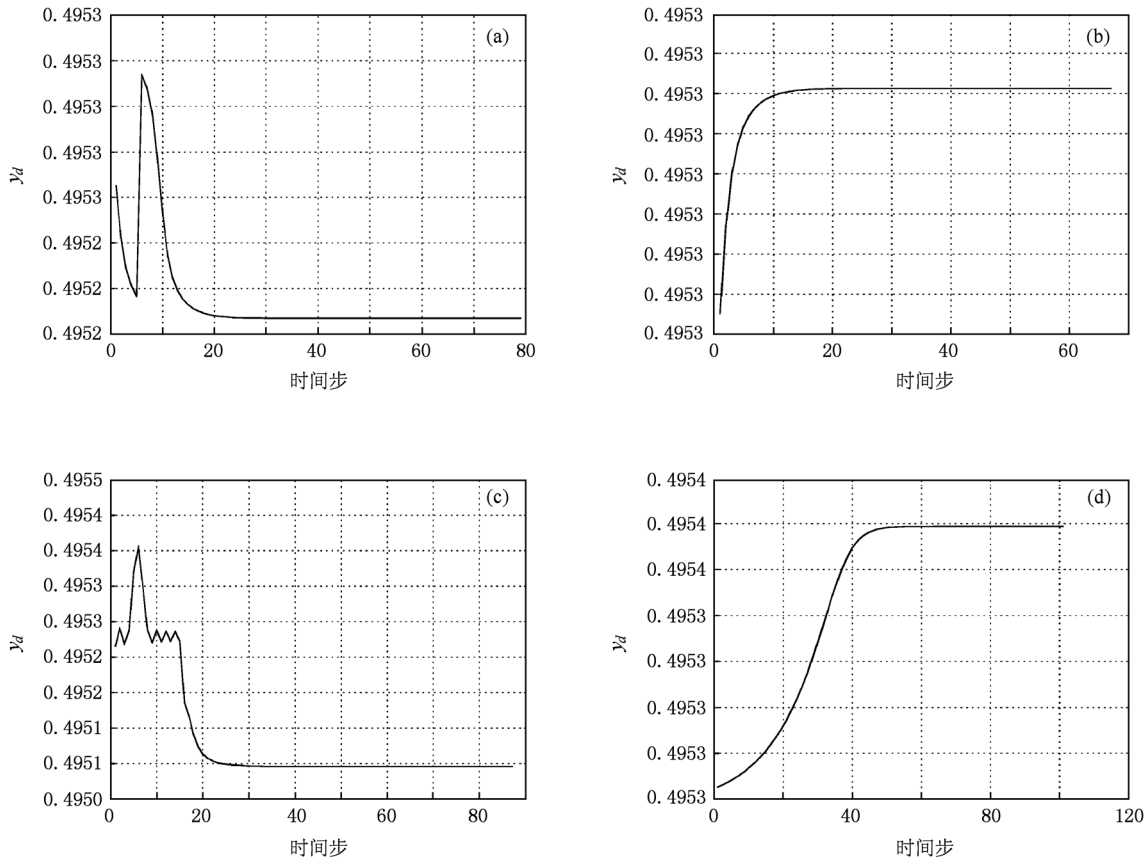

图4 根据(10)式所述的寻优算法寻找常数驱动 y_{d1} 的过程 (a) $b_1 = 0.7865302612$; (b) $b_1 = 0.2167895352$; (c) $b_1 = 0.9622608529$; (d) $b_1 = 0.5142749875$

$g(b_1, y_{d1}) = 0$ 成立,那么就存在着一条包含点 (b_1, y_{d1}) 的直线 $Y = AX + B$, 使得上面所有点 (b^*, y^*) 均满足 $g(b^*, y^*) = 0$. 从(4a)式可知,第一个格点的收敛状态为 $y_1 = \varphi(b_1, y_{d1})$. 根据 $y_i = \phi^{i-1}[\varphi(y_d)]$ 和(9)式可知 $g(b_1, y_{d1})$ 由 y_1 唯一确定. 因此,任意点 (b^*, y^*) 使得 $y_1 \mid_{b=b^*, y_d=y^*} = \varphi(b_1, y_{d1})$ 成立都将有 $g(b^*, y^*) = g(b_1, y_{d1}) = 0$. 根据(4a)式可得直线的方程为

$$y^* = \varphi(b_1, y_{d1})/\varepsilon + \varphi(b_1, y_{d1}) \times (1 - y_1)(1 - \varepsilon)(3.75 + b^*)/\varepsilon. \quad (11)$$

因此,可以用(10)式的迭代算法计算每一个 $b_1 \in [0,1]$ 对应的 y_{d1}, 为了减小计算量取区间 Φ 的中点为迭代算法的起点. 实验结果示于图5,所有满足条件的点 (b^*, y^*) 属于5条直线.

本文中,随机选择 $b_1 = 0.7865302612$ 作为密钥加密一串语音信号. 重构密钥的过程如下:

步骤1 根据(2)式构造一个解密系统,其中密钥 b_1 可以任意选择. 令 $\gamma = 0.0001$, 一旦 b_1 选定,根据(10)式可以计算出相应的 y_{d1}. 重选择密钥并重复上述过程,那么我们就可以得到多组 (b_1, y_{d1}), 根据这些 (b_1, y_{d1}), 可以计算出这5条直线的方程, 5条直线方程的对应参数如表1所示,其中每个数据均由100次平均得到.

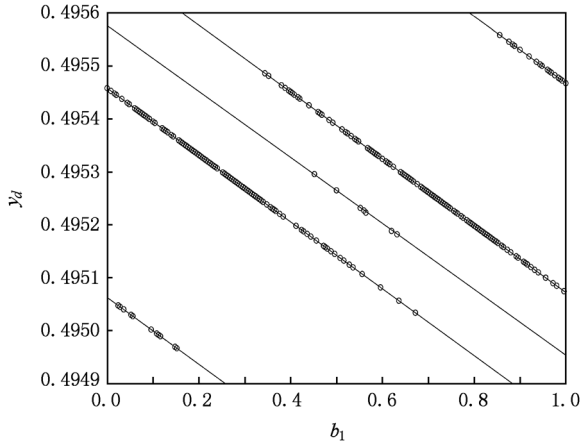

图5 常数驱动 y_{d1} 同测试密钥 b 的关系,满足 $g(b_1, y_{d1}) = 0$

步骤 2 随机选择一个常数作为实际解密系统的输入,利用(10)式,迭代获得相应的 $y_{d1} = 0.495206963987366133$.

步骤 3 将 $y_{d1} = 0.495206963987366133$ 代入上述 5 条直线的方程,并求出对应的五组解: -0.2283274311, 0.3978096430, 0.5934578440, 0.7865302612 和 1.412698303. 显然只有 $\{0.3978096430, 0.5934578440, 0.7865302612\}$ 之一为正确的密钥,因为只有这三个解在[0,1]区间. 因此,如果用这三个密钥构造解密机,必存在一个能够成功解出明文. 实验结果如图 6 所示.

表1 满足条件点 (b^*, y^*) 所组成的 5 条直线的方程

直线	A	B
1	-0.000631312462327782	0.495062818034644914
2	-0.000631313093178722	0.495458106423557865
3	-0.000622651840623326	0.495576481606239128
4	-0.000631313094171622	0.495703510840223460
5	-0.000631312458570371	0.496098818026457278

让我们考虑本算法的计算复杂度和可靠性,本文提出的优化算法大致可以分为三个部分,常数收敛阶段,迭代寻密阶段以及确认密钥阶段. 在常数迭代阶段,如图 1 所示,当驱动信号为常数时,最多不超过 40 步迭代,系统的所有格点均收敛到不动点. 在迭代寻密阶段,为了降低(10)式的迭代算法的计算量,我们选择 Φ 的中点为迭代算法的起点. 当 $\gamma = 0.0001$ 时,如图 4 所示,最多不超过 50 步迭代,即可得到相应的 y_{d1}. 考虑重构密钥的过程可以发现,保证本算法有效的关键是尽可能精确的描述 (b^*, y^*) 所组成的 5 条直线的方程,而这一般通过

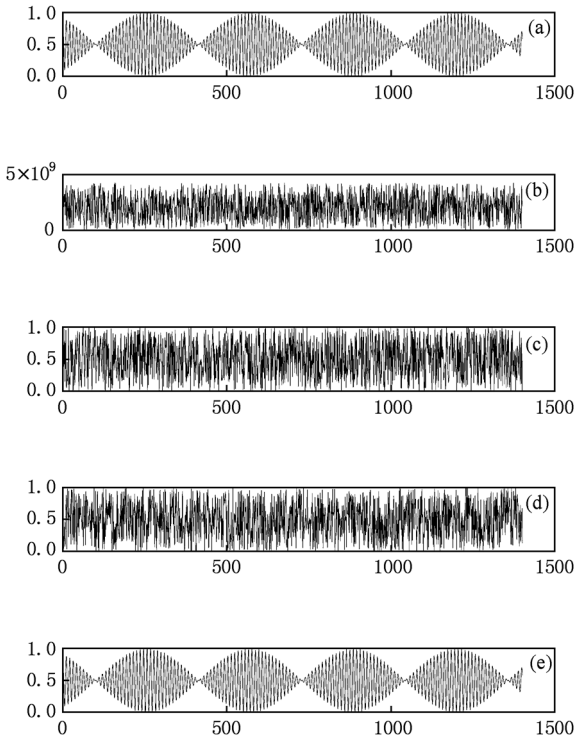

图6 实际攻击结果 (a)明文信息;(b)密文信息;(c)使用错误密钥 0.3978096430 解密后结果;(d)使用错误密钥 0.5934578440 解密后结果;(e)使用正确密钥 0.7865302612 解密后结果

两个方面来保证精确性. 第一:对于通过(10)式的迭代算法得到的每一组 (b_1, y_{d1}),我们都需要重复计算并求取平均值. 如图 4 所述,图中每组数据均为重复计算 100 次的所得的平均值. 第二,我们尽可能多的通过步骤 1 得到相应的 (b^*, y^*) 组合. 如图 5 所示,图中每一个圆点即表示一次通过迭代寻密得到 (b^*, y^*) 的试验结果. 显然,试验结果越多,通过图 5 中各个圆点拟合出的直线越准确. 当我们得到 5 条曲线方程之后,根据重构密钥的过程步骤 2 和步骤 3 可知,根据实际加密系统所对应的 y_{d1},通过表 1 所示直线方程,攻击者至多可得 5 个密钥的可能值,而其中之一必然就是实际密钥. 因此攻击者至多需要尝试 5 次,即可确定的密钥值.

如果我们将(1a)式至(1d)式泛化为一个结构复杂高维混沌,那么可以发现文献[6]所提出的混沌保密系统同样利用符号化混沌序列这一设计思想. 根据(1f)式, N 节点的动力轨迹被符号化为符号序列 K_n 并用以加密明文 I_n. 在解密端,利用混沌同步技术,解密端重构出动力轨迹 $y_n(N)$ 并符号化得到解密密钥流 K', 进而解密密文. 通过符号化操

作：$K_n = \mathrm{int}(x_n(N) \times 2^{\mu}) \bmod 2^{\nu}$，攻击者根据密钥流 K_n 需要 $2^{\mu-\nu}$ 的计算量才能最后一个格点的状态变量 $x_n(N)$，从而保证了原始算法的安全性.

一个理想的混沌伪随机符号序列应该互不相关且均匀分布，任意密钥的选择不能改变伪随机序列的统计特性. 然而控制参数决定序列动力学特性始终是混沌密码学一个本质缺陷[17]. 因此事实上，考虑[8]所提出的混沌保密系统，一旦密钥 b_1 确定(对于混沌系统，则是控制参数 b_1 确定)，那么动力序列 $x_n(N)$，$y_n(N)$ 以及符号序列 K_n，K'_n 的动力特性确定，并且利用 $g(b, y_d)$ 我们可以构建出密钥 b_1 和符号序列 K_n 一一对应关系. 因此可以看出，尽管使用了耦合映像格子以及同步技术，文献[8]所设计的混沌保密系统依然没有避免控制参数决定序列动力学特性这一混沌密码本质缺陷，而这也是当初开展这项安全分析工作的理论依据.

需要指出的是，在后续的改进算法中[9—12]，通过 S-box 操作以及位变换，控制参数和符号序列 K_n，K'_n 间的对应关系更加复杂，很难利用 $g(b, y_d)$ 通过动力序列 $x_n(N)$，$y_n(N)$ 以及符号序列 K_n，K'_n 间的动力特性重构出密钥 b_1 和符号序列 K_n 一一对应关系，因此本文提出攻击方法并不适用后续的改进算法中. 但是由于符号序列 K_n，K'_n 依然由控制参数决定，因此混沌密码本质缺陷就必然存在，在我们后续工作中，我们可以借鉴文献[15]所提出的相关工作，着重研究密钥 $\boldsymbol{b}$ 对密钥流 K_n，K'_n 动力特性的影响，争取文献[8]所提算法及其后续改进算法的攻击策略.

4. 结 论

本文将安全分析文献[8]中所提出的原型自同步的时空混沌流密码系统. 我们发现该高维的加解密系统在常数的驱动下将收敛到一维，使得动力学系统的复杂性大为降低. 在某些特定输入区域内容，保密系统对输入状态的微小扰动不敏感. 而我们可以建立密钥和特殊输入状态间一个简单的线性关系，并依次从密钥流中恢复出密钥. 基于此，我们提出一套攻击方法，利用系统参数和扰动前后密钥流的差异之间的依赖关系通过寻优算法破解密钥，从而攻击了文献[8]所提出了基于混沌自同步的安全通信算法.

[1] Li P, Li Z, Halang W A, Chen G R 2006 *Phys. Lett.* A **349** 467

[2] Li P, Li Z, Halang W A, Chen G R 2006 *Int. J Bifurcation Chaos* **16** 2949

[3] Xiang F, Qiu S S 2008 *Acta Phys. Sin.* **57** 6132 [向 菲、丘水生 2008 物理学报 **57** 6132]

[4] Wang L, Wang F P, Wang Z J 2006 *Acta Phys. Sin.* **55** 3964 [王 蕾、汪芙平、王赞基 2006 物理学报 **55** 3964]

[5] Wang K, Pei W J, Wang S P, Cheung Y M, He Z Y 2008 *IEEE Trans. Circuits Syst. I.* **55** 1116

[6] Wang K, Pei W J, Wang S P, Xia H S, He Z Y 2007 *Acta Phys. Sin.* **56** 3766 [王 开、裴文江、夏海山、何振亚 2007 物理学报 **56** 3766]

[7] Pecora L M, Carroll T L 1990 *Phys. Rev. Lett.* **64** 821

[8] Wang S, Kuang J Y, Li J, Luo Y, Lu H, G. Hu 2002 *Phys. Rev.* E **66** 065202

[9] Tang G N, Wang S H, Lu H P, Hu G 2003 *Phys Lett.* A **318** 388

[10] Ye W P, Dai Q L, Wang S H, Lu H P, Kuang J Y, Zhao Z F, Zhu X Q, Tang G N, Huang R H, Hu G 2004 *Phys Lett.* A **330** 75

[11] Wang X, Gong X, Zhan M, Lai C H 2005 *Chaos* **15** 023109

[12] Zhou J T, Pei W J, Wang K, Huang J, He Z Y 2006 *Phys Lett.* A **358** 283

[13] Lu H P, Wang S H, Li X W, Tang G N, Kuang J Y, Ye W P, Hu G 2004 *Chaos* **14** 617

[14] Wang S H, Hu G 2007 *Chaos* **17** 023119

[15] Rhouma R, Safya B 2007 *Chaos* **17** 033117

[16] Hu G J, Feng Z J, Meng R L 2003 *IEEE Trans. Circuits Syst-I* **50** 275

[17] Wang K, Pei W J, Yi Shen, Wang S P 2009 *Phys. Lett.* A **374** 44

Security of chaos-based secure communications in a large community*

Wang Kai† Pei Wen-Jiang Zhou Jian-Tao Zhang Yi-Feng Zhou Si-Yuan

(*Department of Radio Engineering, Southeast University, Key Laboratory of Underwater Acoustic Signal Processing of Ministry of Education, Southeast University, Nanjing* 210096, *China*)

(Received 24 August 2010; revised manuscript received 8 October 2010)

Abstract

In this paper, we present an attack on a cryptosystem designed by using a spatiotemporal chaotic system. We show that the decryption system proposed in (*Phys. Rev.* E **66**, 065202 (2002)) degenerates to the one-dimensional map under the constant input, and it is insensitive to the slight perturbations to input in specially selected intervals. Consequently, the attacker can use a very simple optimization algorithm to obtain the proper input value within only hundreds of iterations. Furthermore, we prove that there exits a linear dependency between the secret key and the obtained input value, so that the attacker can break this spatiotemporal chaos-based secure communication scheme easily. Both theoretical and experimental results show that the lack of security discourages the use of these cryptosystems for practical application.

Keywords: chaotic encryption, coupled map lattices, cryptanalysis

PACS: 05.45.-a, 05.45.Ra, 05.45.Vx

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60672095, 60972165), the National High Technology Research and Development Program of China (Grant No. 2007AA11Z210), the Doctoral Fund of Ministry of Education of China (Grant Nos. 20100092120012, 20070286004), the Foundation of High Technology Project in Jiangsu Province, the Natural Science Foundation of Jiangsu Province (Grant No. BK2010240), the Special Scientific Foundation for the "Eleventh-Five-Year" Plan of China, the National Torch Plan, and the Excellent Young Teachers Program of Southeast University.

† E-mail: kaiwang@seu.edu.cn