

## 基于树形奇偶机的神经网络同步新学习规则

梁一峰\*, 廖晓峰, 任晓霞

(重庆大学 计算机学院, 重庆 400044)

(\*通信作者电子邮箱 muchenfree@gmail.com)

**摘要:**针对神经密码同步速度慢的问题,基于树形奇偶机(TPM),提出修改权值的新规则,在同步过程中设置队列用来记录每次通信的结果,实时估计两个互相通信的树形奇偶机的同步程度,并根据估计的结果决定权值修改幅度,在同步程度较低时适当增大权值修改量,在同步程度较高时适当减小权值修改量。仿真实验结果表明,应用新学习规则后同步效率提高了80%以上,同时与几种经典学习规则相比,计算开销更小,安全性得到进一步提高。

**关键词:**树形奇偶机;神经网络;同步;神经密码

**中图分类号:**TP309.7 **文献标志码:**A

### New neural synchronization learning rule based on tree parity machine

LIANG Yifeng\*, LIAO Xiaofeng, REN Xiaoxia

(College of Computer Science, Chongqing University, Chongqing 400044, China)

**Abstract:** To solve the low speed of synchronization, a new learning rule was proposed by employing Tree Parity Machine (TPM). By setting queues to record the results of each communication in the synchronization process, this rule estimated the degree of synchronization of the two TPMs communicating with each other in real time. According to the results of estimation, the rule selected appropriate values to modify the weights, appropriately increased weight modifications in the lower degree of synchronization and reduced weight modifications in the higher degree of synchronization. Finally, the simulation results show that synchronization efficiency is improved more than 80% by applying new learning rule. Meanwhile, it is also indicated that the rule is computationally inexpensive and it improves the security of communication compared to the classic learning rules.

**Key words:** Tree Parity Machine (TPM); neural network; synchronization; neural cryptography

## 0 引言

随着计算机网络与信息产业的迅速发展,安全已经成为信息传输和保密通信领域的重要问题。加密是保证信息安全的一种重要手段,通信双方如何快速、高效地协商并产生安全的密钥一直是现代密码学的关键问题。

在公钥密码体制未提出之前,通信双方通过协商一个密钥并长期应用协商好的密钥保持通信,但是这样的方式有着致命的问题,一旦密钥信息泄露或者被攻击者破解,双方很难在短时间内产生新的密钥,同一密钥使用时间越久,安全性就越低。随着密码学的发展,公钥密码体制应运而生。迄今为止,大部分公钥密码体制都是基于某个至今尚未解决的数学难题。通信双方通过公钥密码传输用于通信的会话密钥,这样不仅保证了密钥交换的安全性,同时在必要时可以及时地更新密钥。

2000年,国外学者 Kanter 等提出交互式神经网络并从理论上阐述了其动力学特征<sup>[1-2]</sup>,这种交互式神经网络在密码学中的首次应用是在文献[3]中;文献[4]对这种神经密码作了全面、系统的分析;文献[5]在神经密码中引入了反馈机制;文献[6]提出了有询问机制的神经密码;文献[7]提出了神经同步的判定算法;文献[8-11]分别介绍了几种神经密码的攻击方法,包括简单攻击、几何攻击、主要攻击和遗传攻

击。几种方法都有一定的概率攻击成功,但是随着  $L$  的增大,几种攻击方法成功的概率都迅速收敛到 0。分析结果表明这种密钥协商方法是可行的,并可以抵抗各种已知的攻击方法。因为此模型中只涉及到简单的加法和乘法操作,所以相对公钥密码而言,有着运算速度快和易于在计算机上实现等诸多优点。尽管如此,此模型在通信双方学习的过程中通信次数过多也产生了很大的开销。

本文将在简要介绍神经密码协议的基础上,针对模型达到同步所需通信次数过多的问题,提出相应的解决方案,并用仿真实验给予验证。

## 1 树形奇偶机模型

### 1.1 树形奇偶机结构

树形奇偶机(Tree Parity Machine, TPM)是一种多层前向反馈网络,它的一般结构如图1所示。

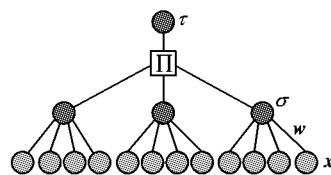


图1  $K=3, N=4$  的 TPM 结构

图1所示神经网络由  $K$  个隐藏单元组成,每个隐藏单元

收稿日期:2012-07-31;修回日期:2012-09-10。

基金项目:国家自然科学基金资助项目(60973114);重庆市自然科学基金重点资助项目(CSTC2009BA2024)。

作者简介:梁一峰(1987-),男,黑龙江绥化人,硕士研究生,主要研究方向:信息安全、人工神经网络;廖晓峰(1964-),男,重庆人,教授,博士,主要研究方向:信息安全、非线性控制理论;任晓霞(1986-),女,山东德州人,硕士研究生,主要研究方向:CNN图像处理、稳定性理论。

有  $N$  个输入和一个输出,所有的输入值都是二值的<sup>[12]1</sup>,即:

$$x_{i,j} \in \{+1, -1\} \quad (1)$$

神经元的权值,用来定义输入与输出之间的映射关系,它们都是从  $-L$  到  $+L$  之间的整数<sup>[12]1</sup>,即:

$$w_{i,j} \in \{-L, -L+1, \dots, +L\} \quad (2)$$

其中: $i$ 表示TPM的第 $i$ 个隐藏单元; $j$ 表示每个隐藏单元的第 $j$ 个元素, $1 \leq j \leq N$ 。

与其他的神经网络类似,隐藏单元的输出由当前输入的加权和决定,第 $i$ 个隐藏单元的输出由 $h_i$ <sup>[12]2</sup>的符号决定,如式(3):

$$h_i = \frac{1}{\sqrt{N}} w_i \cdot x_i = \frac{1}{\sqrt{N}} \sum_{j=1}^N w_{i,j} x_{i,j} \quad (3)$$

即第 $i$ 个隐藏层的输出<sup>[12]2</sup>如式(4):

$$\sigma_i = \text{sgn}(h_i) \quad (4)$$

这里有一个特殊情形,若 $h_i = 0$ ,规定 $\sigma_i = -1$ 来保证 $\sigma_i$ 是二值的。这样,只有在输入值的加权和为正时, $\sigma_i = +1$ ,隐藏单元是活跃的;否则, $\sigma_i = -1$ ,该隐藏单元不活跃。

TPM的最终输出由该TPM的所有隐藏单元的乘积决定<sup>[12]2</sup>,如式(5):

$$\tau = \prod_{i=1}^K \sigma_i \quad (5)$$

显然,不活跃的隐藏单元( $\sigma_i = -1$ )的个数为偶数时 $\tau = +1$ ;为奇数时 $\tau = -1$ 。所以,有 $2^{k-1}$ 种不同的内部值 $\sigma_1, \sigma_2, \dots, \sigma_k$ 可以产生同一个 $\tau$ 。

## 1.2 学习规则

设 $A, B$ 是两个TPM, $A, B$ 在通信开始时分别独立随机产生权值向量 $w^{A,B}$ 。在每一步中,随机产生一个输入向量 $x_i$ 并通过1.1节中的式(3)~(5)计算相应的输出 $\tau^{A,B}$ 。 $A, B$ 将它们的输出与对方交换后,如果 $\tau^A \neq \tau^B$ 则权值不修改;如果 $\tau^A = \tau^B$ ,则选择应用下面的学习规则更新权值。

在Hebbian学习规则<sup>[12]2</sup>中,两个神经网络互相学习,如式(6):

$$w_{i,j}^+ = g(w_{i,j} + x_{i,j} \tau \Theta(\sigma_i \tau) \Theta(\tau^A \tau^B)) \quad (6)$$

$A, B$ 也可以用与它们计算结果相反的值进行学习,这通过anti-Hebbian学习规则<sup>[13]</sup>实现,如式(7):

$$w_{i,j}^+ = g(w_{i,j} - x_{i,j} \tau \Theta(\sigma_i \tau) \Theta(\tau^A \tau^B)) \quad (7)$$

对于 $A, B$ 来说,因为 $\tau^A = \tau^B$ ,所以 $\tau$ 对两个神经网络同步的过程来说并不十分重要,所以也可以应用random-walk学习规则<sup>[14]</sup>,如式(8):

$$w_{i,j}^+ = g(w_{i,j} + x_{i,j} \Theta(\sigma_i \tau) \Theta(\tau^A \tau^B)) \quad (8)$$

当然,应用这些学习规则修正权值的同时要保证结果在规定允许的范围( $-L \sim +L$ ),如果修改后的权值超出了这个范围,则将它重置为最近的边界值 $\pm L$ <sup>[12]2</sup>:

$$g(w) = \begin{cases} \text{sgn}(w) \cdot L, & |w| > L \\ w, & \text{其他} \end{cases} \quad (9)$$

使用式(6)~(8)对权值进行修正,重复以上步骤直至 $A, B$ 的权值相等,即 $w^A = w^B$ 。

从式(6)~(8)可以看出,在以上三种学习规则下,每一次更新权值时,两个TPM中只有那些满足 $\sigma_i = \tau$ 的隐藏单元的权值会发生改变,因此在 $\sigma_1, \sigma_2, \dots, \sigma_k$ 未知的情况下,哪些神经元的权值得到了修正也是不可知的,正是因为这个特性,才使得神经同步在密码学上应用成为可能。

## 1.3 同步度量参数

为了描述两个TPM在同步过程中的同步程度,首先定义隐藏单元权值的概率分布,如式(10):

$$p_{a,b}^i = P(w_{i,j}^A = a \wedge w_{i,j}^B = b) \quad (10)$$

这里 $p_{a,b}^i$ 表示在 $A$ 中有 $w_{i,j} = a$ ,在 $B$ 中有 $w_{i,j} = b$ 的概率,在仿真过程中,度量同步程度的参数可由 $p_{a,b}^i$ 通过式(11)~(13)<sup>[15]</sup>求得:

$$Q_i^A = \frac{1}{N} w_i^A w_i^A = \sum_{a=-L}^L \sum_{b=-L}^L a^2 p_{a,b}^i \quad (11)$$

$$Q_i^B = \frac{1}{N} w_i^B w_i^B = \sum_{a=-L}^L \sum_{b=-L}^L b^2 p_{a,b}^i \quad (12)$$

$$R_i^{AB} = \frac{1}{N} w_i^A w_i^B = \sum_{a=-L}^L \sum_{b=-L}^L ab p_{a,b}^i \quad (13)$$

则两个TPM的对应隐藏单元的同步程度<sup>[15]</sup>可计算如式(14):

$$\rho_i^{AB} = \frac{w_i^A \cdot w_i^B}{\sqrt{w_i^A \cdot w_i^A} \sqrt{w_i^B \cdot w_i^B}} = \frac{R_i^{AB}}{\sqrt{Q_i^A Q_i^B}} \quad (14)$$

两个TPM对应的隐藏单元,在整个同步过程的开始, $\rho_i = 0$ ;当双方达到完全同步状态时, $\rho_i = 1$ 。因此 $\rho_i$ 是分析同步过程的重要参数。

## 2 神经密码学习规则的改进

### 2.1 Hebbian等经典学习规则的局限

实验表明,通过TPM产生密钥,通信双方往往要几千次甚至上万次交换彼此产生的输出值,这样不仅速度慢,开销大,同时可能由于通信时间过长被攻击者攻破的可能性就会增大。本文在原有三种学习规则的基础上,做适当的改进以提高通信的效率,减少通信次数,缩短同步进程。

### 2.2 新学习规则的设计思想

下面以Hebbian学习为例,说明神经密码学习规则的改进方法,此方法同样适用于anti-Hebbian学习规则和random-walk学习规则。

本文在Hebbian学习的基础上适当地调整权值修改的幅度来加快学习的进程。 $\rho$ 是判断神经网络同步程度的重要参数,神经网络同步的过程也就是 $\rho$ 不断增大最终达到1的过程,因为只有在 $A$ 和 $B$ 输出结果 $\tau^A = \tau^B$ 才进行学习,如果 $w^A$ 和 $w^B$ 的同步程度较高,那么对于一个随机输入的 $X, A, B$ 产生的输出相同的概率就较大;否则如果 $w^A$ 和 $w^B$ 的同步程度较低, $A, B$ 产生的输出相同的概率就较小。因此, $A, B$ 可以分别在学习过程中设置一个队列来记录最近一段时间内 $A, B$ 的通信结果,即 $\tau^A = \tau^B$ 的次数和 $\tau^A \neq \tau^B$ 次数,每次需要修改权值时,通过计算队列中 $\tau^A \neq \tau^B$ 占整个队列的比例决定权值修改量的大小,如果 $\tau^A \neq \tau^B$ 的比率较大,说明 $A$ 和 $B$ 的同步程度较低,则增大权值修改量;否则,减小权值修改量。

### 2.3 神经同步学习新规则

具体修改权值的新规则设计如式(15):

$$w_{i,j}^+ = g(w_{i,j} + \delta\text{step} * x_{i,j} \tau \Theta(\sigma_i \tau) \Theta(\tau^A \tau^B)) \quad (15)$$

新学习规则(15)与Hebbian学习规则相比,在权值修改的幅度上是原来的 $\delta\text{step}$ 倍, $\delta\text{step}$ 由式(16)求出:

$$\delta\text{step} = \lfloor 1 + \text{sum} * L / \text{queue.length} \rfloor \quad (16)$$

其中: $\text{sum}$ 表示队列中记录的 $\tau^A \neq \tau^B$ 的次数, $\text{queue.length}$ 表示队列长度, $\lfloor \cdot \rfloor$ 表示向下取整。

这里 $\delta\text{step}$ 的计算采用 $\lfloor 1 + \dots \rfloor$ 的形式,是因为当两个TPM即将达到同步时但 $w^A \neq w^B$ 时,很有可能队列中的记录

的所有通信结果都是  $\tau^A = \tau^B$ , 这样  $\tau^A \neq \tau^B$  的次数就为 0, 于是  $\text{sum} * L / \text{queue.length} = 0, +1$  并向下取整是为了保证在每次需要更新权值时, 修改量至少为 1。

本文主要工作就是对神经网络同步过程中的学习规则在已有学习规则(以 Hebbian 学习规则为例)的基础上进行了改进, 每次通信过程中两个 TPM 的输出的计算方法与 1.1 节中的描述相同, 在权值需要更新时采用式(15)~(16)进行更新。

### 3 仿真实验结果

#### 3.1 新学习规则下队列长度的确定

为了观察队列长度对同步速度的影响, 在本文设计的新学习规则下, 做了 1000 次模拟仿真实验, 实验结果如图 2。从图 2 可知, 在  $K=3, N=1000$  时对不同的  $L$  值实验分别选取了队列长度为  $L, 2L, 3L, 4L, 5L$ , 实验结果显示, 队列长度为  $L$  的同步曲线整体处于队列长度为其他值的同步曲线的下方, 即当队列长度为  $L$  时应用新规则同步速度最快, 因此, 在后面的应用新规则的仿真实验中, 本文一致选取队列长度为  $L$ 。从图 2 中不难得出, 当队列长度较长时, 同步速度有所下降, 这是因为当队列长度较长时, 在计算  $\delta\text{step}$  的过程中, 较多地考虑了先前的通信结果, 以致降低了对当前状态下两个 TPM 同步程度判断的准确性, 因此, 适当地选取队列长度是十分必要的。

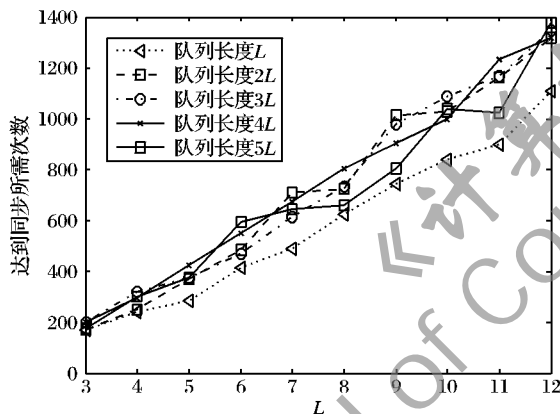


图2 队列长度与同步所需次数关系 ( $K=3, N=1000$ )

#### 3.2 新规则下同步性能和安全性能分析

图 3 给出了在  $K=3, N=1000$  时, Hebbian 学习规则和新学习规则同步所需次数与  $L$  的关系, 新规则下同步所需次数比 Hebbian 学习规则下同步所需次数减少了 80% 以上, 即新规则下同步性能比 Hebbian 学习规则提高了 80% 以上。新规则下权值修改量与  $\rho$  的关系如图 4 所示, 本文做了 100 次仿真实验, 从图 4 可以看出, 新规则下, 在同步程度较低时, 权值修改量较大, 而在同步过程接近尾声时, 权值修改量较小, 实验结果完全符合预期, 这也说明, 本文采用的在同步过程中设置队列来记录同步过程并实时估算同步程度的方法是行之有效的。应用 Hebbian 学习规则和新学习规则在同步速度上更直观的比较结果如图 5 所示, 在  $K=3, N=1000, L=30$  时, Hebbian 学习规则达到同步所需的通信次数约为  $3.2 \times 10^4$ , 新学习规则下  $\rho$  收敛到 1 的速度明显更快, 达到同步所需的通信次数约为  $0.4 \times 10^4$ , 效率提高了 80% 以上。同时, 新规则下产生的空间开销(设置长度为  $L$  的队列)很小, 时间开销(计算  $\delta\text{step}$  的时间)与同步过程中的计算量相比可以忽略。

综上所述, 新学习规则在同步速度上比 Hebbian 学习规则有较大的提高。同时, 图 6 给出了在  $K=3, N=1000$ ,

$L=30$  时 Hebbian 学习规则和新学习规则在仿真实验下达到同步时的权值分布对比。实验结果表明, 新学习规则适当地增大权值修改量对权值的分布影响并不大, 因此, 新学习规则既加快了同步的速度, 同时并没有损失安全性, 甚至由于速度加快, 更加大了攻击者攻破的难度。

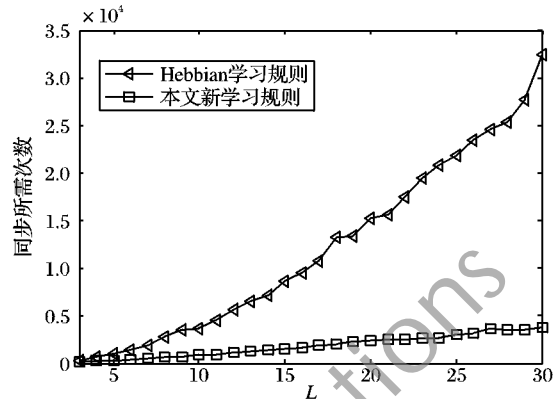


图3 两种学习规则同步速度对比 ( $K=3, N=1000$ )

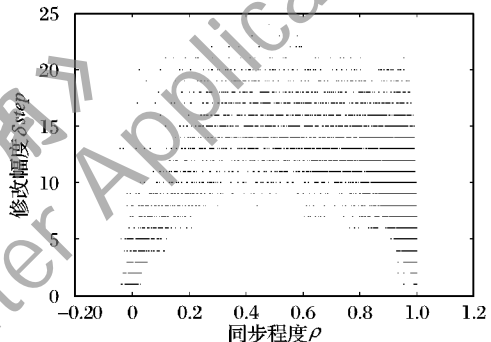


图4 新学习规则下  $\rho$  与权值修改幅度  $\delta\text{step}$  的关系

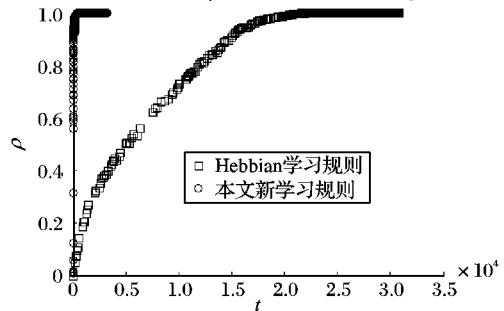


图5  $K=3, N=1000, L=30$  时  $\rho$  与同步时间  $t$  的关系

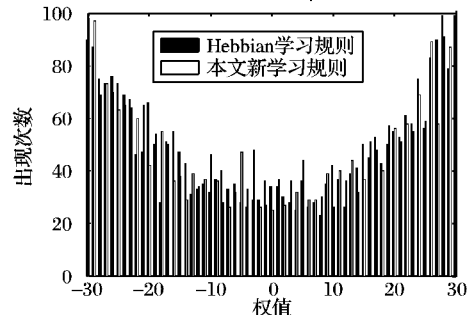


图6  $K=3, N=1000, L=30$  时同步后权值分布直方图

### 3 结语

本文指出了神经密码同步速度慢的问题, 提出了改进的方法, 并通过大量的仿真实验验证, 在此基础上, 对安全性和效率进行了分析。使用新学习规则后, 同步时间明显缩短, 不仅减少了通信开销同时提高了安全性。

(下转第 152 页)

按照用户权限隔离的目标,每个用户的访问行为只能被该类用户的访问授权序列对应的自动机所识别,其他权限不同用户的自动机是无法识别这种访问行为的。而定理3则说明,不同用户对权限交集部分的访问,可以被所有这些用户访问授权序列对应的自动机接受。从模型的公式推导上来看这是正确的,且在现实系统中也确实存在这样的应用场景,例如一个普通用户和一个管理员用户都可以访问 mail 服务,但是操作系统中一旦某个用户因为某种操作提升了自己的权限,其所有的访问行为都有可能被权限不同的用户对应的自动机所接受,如普通用户由于系统服务的漏洞获取了管理员权限,就可以以管理员身份对 mail 服务进行任意的操作,并且这些操作都能被操作系统所接受,即都被认为是合法的。这也证明了本文引言中所提出的由于共享所导致的权限问题。

### 3 结语

本文提出了基于有限状态机的用户权限隔离模型,将用户的授权访问行为刻画为一个有限状态机,任意用户的有限状态机都只能识别该用户的合法操作序列,不能识别其他用户的操作行为,并指出在用户权限交集的部分,即用户访问发生共享的点,容易出现权限窃取或者非法提升等问题。最终,利用有限状态机实现了对用户操作权限隔离的描述,并能够对这种隔离进行有效识别与判定。

#### 参考文献:

- [1] 沈昌祥,张焕国,冯登国,等.信息安全综述[J].中国科学E辑:信息科学,2007,2(1):129-150.
- [2] SALTZER J H, SCHROEDER M D. The protection of information in computer systems [J]. Proceedings of IEEE, 1975, 63(9): 1278-1308.
- [3] BUYENS K, de WIN B, JOOSEN W. Resolving least privilege violations in software architectures [C]// Proceedings of the 5th International Workshop on Software Engineering for Secure Systems. Washington, DC: IEEE Computer Society, 2009: 9-16.
- [4] LEVIN T E, IRVINE C E, NGUYEN T D. A least privilege model for static separation kernels, NPS-CS-05-003 [R]. Monterey: Naval Postgraduate School, Center of Information Systems Security Studies and Research, 2004.
- [5] 梁彬.可信进程机制及相关问题研究[D].北京:中国科学院软件研究所,2004.
- [6] CHEN S, DUNAGAN J, VERBOWSKI C, et al. A black-box tracing technique to identify causes of least-privilege incompatibilities [EB/OL]. [2012-06-10]. <http://www.isoc.org/isoc/conferences/ndss/05/proceedings/papers/chen-ndss05.pdf>.
- [7] 朱鲁华.安全操作系统模型和实现结构研究[D].郑州:信息工程大学,2002.
- [8] FERRAILOLO D F, KUHN D R. Role-based access control [C]// Proceedings of the 15th NIST-NSA National Computer Security Conference. Baltimore, MD: [s. n.], 1992: 554-563.
- [9] SANDHU R S, COYNE E J, FEINSTEIN H L, et al. Role-based access control models [J]. Computer, 1996, 29(2): 38-47.
- [10] FERRAILOLO D F, CUGINI J, KUHN D R. Role-Based Access Control (RBAC): features and motivations [C]// Proceedings of the 11th Annual Computer Security Applications Conference. Washington, DC: IEEE Computer Society, 1995: 241-248.
- [11] KUHN D R. Mutual exclusion of roles as a means of implementing separation of duty in role-based access control systems [C]// Proceedings of the 2nd ACM Workshop on Role-based Access Control. New York: ACM Press, 1997: 23-30.
- [12] CHEN H, LI N H. Constraint generation for separation of duty [C]// Proceedings of the Eleventh ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2006: 130-138.
- [13] 徐小良,汪乐宇,周泓.有限状态机的一种实现框架[J].工程设计学报,2003,10(5):251-255.

(上接第148页)

神经密码是近10年才兴起的研究方向,它有着自己独特的特点,算法简单,易于实现,同时它与公钥密码理论不同,不需要很高的数学水平,入门容易,相信不久的将来,神经密码会发展成为密码学的重要分支学科。

#### 参考文献:

- [1] METZLER R, KINZEL W, KANTER I. Interacting neural networks [J]. Physics Review E, 2000, 62(2): 2555-2565.
- [2] KINZEL W, METZLER R, KANTER I. Dynamics of interacting neural networks [J]. Journal of Physics A: Mathematical and General, 2000, 33(14): L141-L147.
- [3] KINZEL W, KANTER I. Interacting neural networks and cryptography [M]// KRAMER B. Advances in Solid State Physics. Berlin: Springer, 2002, 42: 381-391.
- [4] ROSEN-ZVI M, KANTER I, KINZEL W. Cryptography based on neural networks—analytical results [J]. Journal of Physics A: Mathematical and General, 2002, 35(47): L707-L713.
- [5] RUTTOR A, KINZEL W, SHACHAM L, et al. Neural cryptography with feedback [J]. Physics Review E, 2004, 69(4): 046110.
- [6] RUTTOR A, KINZEL W, KANTER I. Neural cryptography with queries [J]. Journal Statistical Mechanics: Theory and Experiment, 2005, 2005(1): 01009.
- [7] 田勇,向涛.神经网络同步的判定及在神经密码中的应用[J].计算机工程与应用,2011,47(36):109-111.
- [8] KANTER I, KINZEL W, KANTER E. Secure exchange of information by synchronization of neural networks [J]. Europhysics Letters, 2002, 57(1): 141-147.
- [9] KLIMOV A, MITYAGUINE A, SHAMIR A. Analysis of neural cryptography [C]// ASIACRYPT'02: Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology. Berlin: Springer, 2003: 823-828.
- [10] SHACHAM L N, KLEIN E, MISLOVATY R, et al. Cooperating attackers in neural cryptography [J]. Physics Review E, 2004, 69(6): 066137.
- [11] RUTTOR A, KINZEL W, NAEH T, et al. Genetic attack on neural cryptography [J]. Physics Review E, 2006, 73(3): 036121.
- [12] MISLOVATY R, PERCHENOK Y, KANTER I, et al. Secure key-exchange protocol with an absence of injective functions [J]. Physics Review E, 2002, 66(6): 066102.
- [13] BORNHOLDT S, SCHUSTER H G. Handbook of graphs and networks: from the genome to the Internet [M]. Weinheim: Wiley-VCH, 2005: 199-216.
- [14] KINZEL W, KANTER I. Neural cryptography [C]// Proceedings of the Ninth International Conference on Neural Information Processing. Washington, DC: IEEE Computer Society, 2002: 1351-1354.
- [15] ENGEL A, van den BROECK C. Statistical mechanics of learning [M]. London: Cambridge University Press, 2001: 14-32.