

密钥交换协议研究综述

网络空间安全 赵正一

摘要

密钥交换协议是密码学研究的主要问题之一，通过某种机制通信双方建立联系，并沟通会话密钥。传统的密钥交换协议是基于代数数论建立的，其中比较经典的是由 Diffie 和 Hellman 提出的密钥交换协议。但是这一协议极容易收到中间人攻击，使得通信双方构建的通信通道不再安全。近些年来，神经密码学的提出给密钥交换协议提供了一种新的思路。通信双方构建相同的神经网络框架，通过相互学习机制更新彼此的权重，最终达成权重相等，完成会话密钥的分发。本文介绍了神经密码学在密钥交换协议中的应用，分析了神经密码学的安全性，并对未来工作的发展提出了建议。

关键字： 密钥交换协议；神经密码学；树奇偶校验机

Abstract

Key exchange protocol is one of the main issues in cryptography research. Through a certain mechanism, communication parties establish contact and communicate session keys. The traditional key exchange protocol is based on algebraic number theory, and the more classic one is the key exchange protocol proposed by Diffie and Hellman. However, this protocol is extremely vulnerable to man-in-the-middle attacks, making the communication channel constructed by both parties no longer secure. In recent years, the proposal of neural cryptography has provided a new way of thinking for key exchange protocols. The communication parties construct the same neural network framework, update each other's weights through a mutual learning mechanism, and finally achieve equal weights and complete the distribution of the session key. This paper introduces the application of neural cryptography in key exchange protocols, analyzes the security of neural cryptography, and makes suggestions for the development of future work.

Keywords: Key Exchange Protocol; Neural Cryptography; Tree Parity Machine

目录

1	密码基础知识简介.....	1
2	应用场景及研究现状	1
3	关键技术介绍	2
3.1	TPM 构建.....	2
3.2	TPM 学习规则.....	2
3.3	收敛性分析.....	3
3.4	安全性分析.....	4
3.4.1	暴力破解	4
3.4.2	模拟攻击	5
4	下一步工作.....	5

1 密码基础知识简介

密钥交换是现代密码学通信双方交换密钥以供后续某种加密算法的一个过程，构建一个安全的密钥交换协议对于密钥交换来说至关重要。其中，最为经典的就是 Diffie-Hellman 密钥交换协议（DH 密钥交换协议）。它可以让双方在完全接受窃听者窃听的情况下，完成对会话密钥的共享，并且由于数学困难性，窃听者无法推断出共享会话密钥的详细内容。通过这一密钥交换协议，通信双方可以构建一个安全的通信通道来加密通信内容。

假定 Alice 和 Bob 决定选用 DH 密钥交换协议进行密钥交换，他们将遵循以下算法：

Algorithm 1 DH 密钥交换协议

- 1: Alice 和 Bob 协商一个质数 p 和它的一个生成元（原根） g ；
 - 2: Alice 选择一个秘密数字 a ，计算 $A = g^a \bmod p$ 并发送给 Bob；
 - 3: Alice 选择一个秘密数字 b ，计算 $B = g^b \bmod p$ 并发送给 Alice；
 - 4: Alice 计算 $s_{Alice} = B^a \bmod p$ ，Bob 计算 $s_{Bob} = A^b \bmod p$
-

但它极易受到中间人攻击。窃听者 Eve 在信道的中央进行两次 DH 密钥交换，一次和 Alice，另一次和 Bob。就可以成功的向 Alice 假装自己是 Bob，并向 Bob 假装自己是 Alice。因此通常都需要一个能够验证通讯双方身份的机制来防止这类攻击。

2 应用场景及研究现状

与传统的基于数论的密码学不同，神经密码学是基于神经网络中的同步现象来构建密钥交换协议的。此外，神经密学可以确保窃听者无法推断出密钥，即使窃听者知道算法的全部细节并且可以监听通信通道。通过共享相同的神经网络结构（称为树奇偶校验机，TPM），参与密钥交换协议的两个实体可以通过同步共享神经网络来共享密钥。

通过近几年的发展，已经对神经密码学进行了广泛的研究。Mislovaty 团队证明了通过相互学习机制，可以实现两个树奇偶校验机的同步。这一同步现象表明了树奇偶校验机的同步可以用作密钥交换协议。

从这一结果开始，有人后续分析了整个树奇偶校验机结构中的同步过程，并提出了两个主要的作用方式：相互吸引和相互排斥阶段。通过这两个步骤的不断叠加，可以验证同步发生的确定性，并且证明了同步时间仅取决于设定的深度。

为了在实际中使用基于神经密码学的密钥交换协议，有人提出了扩展的各种概念。最为经典的一个思路是为树奇偶校验机增加认证模块，通过秘密边界实现了带有身份认证的密钥交换协议，保证了树奇偶校验机不会收到中间人攻击。

3 关键技术介绍

树奇偶校验机 (Tree Parity Machine, TPM) 由 K 个隐藏单元组成, 其输入向量是 X , 初始权重是 W , 输出单元是 σ_k :

$$\begin{aligned} X &\subset x_{ij} \in \{-L, \dots, 0, \dots, +L\} \\ W &\subset w_{ij} \in \{-L, \dots, 0, \dots, +L\} \\ \sigma_k &= \text{sign}\left(\sum_{j=1}^N w_{kj} x_{ij}\right) \end{aligned} \quad (1)$$

其中, $\text{sign}(\cdot)$ 函数代表取自变量的数学符号, 用来表示自变量的正负形, 所以有:

$$\text{sign}(\cdot) \in \{-1, 0, +1\}$$

TPM 最终的输出为 τ :

$$\tau^{A/B} = \prod_{k=1}^K \sigma_k^{A/B} \quad (2)$$

3.1 TPM 构建

TPM 的构建是一个动态的过程, 通过多轮对比最终构建并同步好彼此的神经网络。其构建流程如下:

Algorithm 2 TPM 双方同步按照以下流程执行

- 1: 随机初始化权重矩阵 $w_{ij}^{A/B}$;
 - 2: **while** $w_{ij}^A \neq w_{ij}^B$ **do**
 - 3: 随机生成相同的输入矩阵 x_{ij} ;
 - 4: 计算 $\sigma_i^{A/B}$ 和 $\tau^{A/B}$ 的结果;
 - 5: **for all** τ^A 和 τ^B , 比较他们的结果, 并按照如下结果继续执行 **do**
 - 6: $\tau^A = \tau^B$: 更新彼此的权重;
 - 7: $\tau^A \neq \tau^B$: 回到第三步;
 - 8: **end for**
 - 9: **end while**
-

3.2 TPM 学习规则

如 2.2.1 中的流程图所示, 在进行到第 6 步的时候, 需要按照特定的规则来更新神经网络的权重, 通常会使用以下三种更新方法:

1. Hebbian 算法

$$w_i^+ = g(w_i + \sigma_i x_i \theta(\sigma_i, \tau^A) \theta(\tau^A, \tau^B)) \quad (3)$$

2. Anti-Hebbian 算法

$$w_i^+ = g(w_i - \sigma_i x_i \theta(\sigma_i, \tau^A) \theta(\tau^A, \tau^B)) \quad (4)$$

3. Random walk 算法

$$w_i^+ = g(w_i + x_i \theta(\sigma_i, \tau^A) \theta(\tau^A, \tau^B)) \quad (5)$$

其中, $\theta(x, y)$ 代表了 x 和 y 的相等关系, g 函数表示某种运算法则使得运算后的结果仍然保持在原运算空间内:

$$\theta(x, y) = \begin{cases} 1, & x = y \\ 0, & x \neq y \end{cases} \quad (6)$$

3.3 收敛性分析

通过上述公式可以得到, 如果双方的最终输出 $\tau^A = \tau^B$, 而且对于每一个神经网络来说, 每个 $\tau = \sigma_k$ 的神经元都有且只可能有以下三种运动情况:

共同运动 如果同一位置上隐藏层的输出是相等的, 那么 Alice 和 Bob 双方的神经网络对应的神经单元都会发生权重更新, 而且由于每一轮的输入矩阵是相同的, 在相同的运算法则下, 他们的运动方向一定是同向的。

$$\sigma_k^A = \sigma_k^B = \tau^{A/B} \quad (7)$$

某一方单独运动 如果同一位置上隐藏层的输出是不等的, 那么 Alice 和 Bob 双方的神经网络对应的神经单元只有一方会发生权重更新。

$$\sigma_k^A \neq \sigma_k^B \quad (8)$$

不运动 如果同一位置上隐藏层的输出是相等的但是都不等于最终的数据结果, 那么 Alice 和 Bob 双方的神经网络对应的神经单元都不会发生权重更新, 他们不做运动, 或者也可以近似看作他们的运动方向是同向的。

$$\sigma_k^A = \sigma_k^B \neq \tau^{A/B} \quad (9)$$

在此基础上，我们可以定义两个神经单元的距离。本文把同一位置上不同神经网络的隐藏单元看作是在同一条直线上运动的两个动点。由上面的运动情况分析有，他们要么同向运动，要么一方不运动，另一方运动。我们定义两点之间的距离为：

$$\rho_k = \frac{w_k^A \cdot w_k^B}{\sqrt{w_k^A \cdot w_k^A} \cdot \sqrt{w_k^B \cdot w_k^B}} \quad (10)$$

其中， $0 < \rho_k < 1$ 。当 $\rho_k = 0$ 的时候，我们认为动点处于开始位置；当 $\rho_k = 1$ ，我们认为同步结束，双方的权重矩阵相等。

因为神经网络的隐藏单元的深度 L 是一定的，所以对于上述我们简化撑的直线上两动点运动这个模型来说，动点的运动是有边界的。进入边界后，如果继续同向运动，动点被边界吸收，如果与边界反向运动，动点被边界反射。



图 1: 动点运动近似模拟模型

所以两动点的运动长度可以近似为 $m = 2L + 1$ 。故两动点一定会相遇，而且相遇的可能仅与时间相关。所以通信双方使用相同规模的神经网络，在一定时间内的相互学习后，权重矩阵一定会相等。

3.4 安全性分析

安全性分析的条件是，在每一次由 Eve 发起的攻击中，都认为 Eve 可以在 Alice 和 Bob 之间窃听消息，但没有机会更改他们。在这个条件下，我们讨论暴力破解和模拟攻击。

3.4.1 暴力破解

对于一个输入矩阵规模为 $K \times N$ 的输入，隐藏层的权重矩阵 W 的规模为 K ，权重矩阵和输入矩阵的深度都是 L 。在这样的条件下，一共有 $(2L + 1)^{KN}$ 种会话密钥的可能性。假设当前神经网络仅仅是一个 $K = 3$, $N = 100$, $L = 3$ 的模型，它的计算规模也已经达到了 3×10^{253} 。这对于目前的计算能力来说，暴力破解是不可能的。

3.4.2 模拟攻击

模拟攻击建立在窃听者 Eve 建立了一个与 Alice 和 Bob 相同的神经网络，并且在 Alice 与 Bob 的通信交流过程中全程窃听并记录下了内容。试图通过与 Alice 或 Bob 一起更新权重以达到三者权重相同的目的。下面我们分析这种攻击的可能性。

在这样的情况下，攻击者 Eve 一共有三种可能的选择：

1. $\tau^A \neq \tau^B$ ：三方均不更新权重。
2. $\tau^A = \tau^B = \tau^E$ ：Alice 和 Bob 双方因为具有相同的更新条件，所以采用约定好的更新规则更新权重。Eve 因为自身的结果和 Alice 以及 Bob 相等，所以 Eve 也根据窃听到的更新权重规则更新自己的权重。
3. $\tau^A = \tau^B \neq \tau^E$ ：Alice 和 Bob 双方因为具有相同的更新条件，所以采用约定好的更新规则更新权重。但是 Eve 的结果并不相同，所以 Eve 不更新自己的权重。

事实证明，由于概率存在，所以 Eve 的更新效率要远低于 Alice 和 Bob 双方更新权重的效率。所以 Eve 概率上永远也无法先于 Alice 或 Bob 同步权重。

4 下一步工作

神经密码学现在仍然很难应用到工业设计中，因为它本身原理不是基于数学困难性而是基于概率发生的，所以无法保证一定不能通过模拟攻击破解。同时，由于神经密码学在结果交流中仍然要反复利用网络传播，所以无法保证通信效率。在未来，可以通过扩展树奇偶校验机，在保持效率的同时提高结构的安全性。

参考文献

- [1] Allam A M, Abbas H M, El-Kharashi M W. Authenticated key exchange protocol using neural cryptography with secret boundaries[C]//The 2013 International Joint Conference on Neural Networks (IJCNN). IEEE, 2013: 1-8.
- [2] Singh A, Nandal A. Neural cryptography for secret key exchange and encryption with AES[J]. PDF). International Journal of Advanced Research in Computer Science and Software Engineering, 2013, 3(5): 376-381.
- [3] Kinzel W, Kanter I. Neural cryptography[C]//Proceedings of the 9th International Conference on Neural Information Processing, 2002. ICONIP'02. IEEE, 2002, 3: 1351-1354.
- [4] Modesitt D, Henry T, Coden J, et al. Neural Cryptography: From Symmetric Encryption to Adversarial Steganography[J]. Available at <https://courses.csail.mit.edu/6.857/2018/project/Modesitt-Henry-Coden-Lathe-NeuralCryptography.pdf>.
- [5] Abadi M, Andersen D G. Learning to protect communications with adversarial neural cryptography[J]. arXiv preprint arXiv:1610.06918, 2016.
- [6] Jeong S, Park C, Hong D, et al. Neural Cryptography Based on Generalized Tree Parity Machine for Real-Life Systems[J]. Security and Communication Networks, 2021, 2021.