文章编号：2096-1618(2019)05-0449-08

适用于侧信道分析的卷积神经网络结构的实验研究

黄 洁，王 燚
(成都信息工程大学网络空间安全学院，四川 成都 610225)

摘要：侧信道分析中，对模板攻击的模板建立研究已经从高斯分布转变到使用机器学习算法来建立模板。比如使用支持向量机、神经网络等。但是使用神经网络进行侧信道分析时，网络结构的设计参数众多，找到合适的网络结构很困难。基于大量的实验研究，总结并提出适用于侧信道分析的卷积神经网络结构的经验，为今后设计侧信道攻击中的卷积神经网络提供依据。

关 键 词：侧信道分析；模板攻击；卷积神经网络
中图分类号：TN911 **文献标志码**：A
doi：10.16836/j.cnki.jcuit.2019.05.001

0 引言

侧信道分析攻击是利用加密设备在运行过程中的时间消耗、功率消耗等泄露的敏感信息对密钥进行攻击的一种方法。它有多种实现的方式[1-3]，简单能量分析攻击(simple power analysis，SPA)[4]和差分能量分析攻击(differential power analysis，DPA)[5]可归为无学习的攻击方式，模板攻击(template attack，TA)[6]可归为有学习的攻击方式。其中，模板攻击的方法主要分两部分：分析能迹建立模板和实施攻击。在攻击效率上，模板攻击建立了针对泄露信息的能耗模型，攻击时只需要较少的攻击能迹就能成功。在模板攻击中，模板主要通过多元高斯分布来建立，通过将能量迹与多元高斯分布的模板进行匹配，从而识别正确的密钥。模板攻击除了这种经典的方式建立模板外，还有使用机器学习算法来建立模板的方式，比如贝叶斯分类算法[7]、支持向量机[8]、神经网络[9]等。

在机器学习算法中使用神经网络进行侧信道分析主要有多层感知器(multi-layer perceptrons，MLP)[10-12]和卷积神经网络(convolutional neural networks，CNN)[13-14]这两种方式。Martinasek等[10-12]将基于MLP的方法同基于其他方法的模板攻击进行了对比。研究表明，MLP的效果要远远超过其他攻击方式。Eleonora等[13]提出CNN对具有抖动防御的加密算法攻击的有效性。这一研究表明，抖动防御在卷积神经网络模型下失效，但文献中没有给出神经网络的超参数(即网络的层数、大小以及训练采用的优化方法、学习率、训练批大小等)。文献[14]针对这一方法进一步研究，并公开了一组具有抖动防御的能迹集(ASCAD)供研究者使用。ASCAD数据攻击目标泄露的信息非常微弱，因此设计适当的网络结构是非常困难的。文中详细介绍了其设计“最佳”卷积神经网络结构的过程和所得到的最佳网络结构参数。采用的研究方法是每次只调整一个参数，固定其他参数，通过多次训练和攻击，找到该参数的最佳值，然后固定该超参数，再测试下一个超参数。然而超参数对训练效果的影响不是相互独立的。在其余参数给定的情况下测试得到的一个最佳超参数，但在其余参数变化后，该参数将不再是最佳的。文中使用的CNN结构是基于VGG16的。这种卷积网络结构在图像识别中表现出色，实验证明它在能迹建模中并不适用。

神经网络调参是深度学习中广泛存在的一个难题。事实上并不存在针对各类数据均适用的网络结构。文中研究工作目标是寻求针对侧信道的能耗数据，找出有效卷积神经网络的结构设计经验。通过大量的实验，分析出一些设计卷积神经网络结构的经验性原则。例如：信噪比越差，卷积输出特征应该越小；泄露信息越少，首层卷积需要使用更大的卷积核；对能耗数据不宜采用过深的卷积网络；对抖动严重的能迹，卷积网络中应选择最大池化，而非平均池化。

1 背景知识

1.1 卷积神经网络结构及原理

卷积神经网络是一种多层神经网络，一般由卷积层、池化层和全连接层组成。卷积层采用卷积处理提

收稿日期：2019-03-13
基金项目：“十三五”国家密码发展基金资助项目(MMJJ20180244)；国家科技重大专项基金资助项目(2014ZX01032401)；四川省教育厅重点科研基金资助项目(17ZB0082)；四川省重点研发资助项目(2019YFG0096)

取数据的局部特征,并通过多个卷积层提取数据更加抽象的特征。池化层用于数据的降维处理。全连接层是对卷积得到的特征进行融合,并且对特征的概率进行一个判断。

卷积网络的结构如图 1 所示。在卷积层上一般都包含着多个特征平面,在输入层上的一个窗口 W,通过卷积操作得到特征层上的一个特征。窗口 W 移动的距离称为步长。窗口通过移动步长进行卷积得到特征层上其他的特征。但特征层上的特征并不是每一个都有效,通过将特征层上特征 P 进行池化处理得到一个更有效的特征(如图 1 所示的 Pooling Layer)。这样处理也降低了模型的复杂度。卷积和池化层提取得到的数据特征最终在全连接层进行非线性组合,输出数据针对各类别的概率分布。

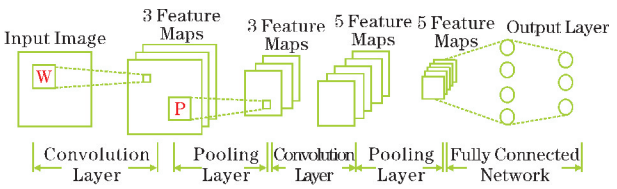


图 1 卷积网络结构

1.2 有学习的侧信道攻击原理

主要使用卷积神经网络作为模板进行学习,得到密钥的操作为

$$K^* = \arg\max_k \prod_{j=1\cdots m} CNN(e_j \mid comb(x_j,k)) \quad (1)$$

其中 K^* 表示正确密钥,$CNN(e \mid comb(x,k))$ 表示训练过程中学习到的分类器模型。

1.3 实验中采用的指标

实验中采用了两个指标来衡量模型训练的效果和使用模型实施攻击的效果。这两个指标分别是模型训练的验证精度和攻击时的猜测熵。模型训练的验证精度是机器学习中常用的指标,表达了模型对数据的分类能力。这一指标在传统的机器学习领域(如图像识别)往往直接体现了模型实现其应用目标的能力(如识别图像类别的能力)。但在侧信道攻击中,数据分类并非模型的最终目标。其最终目标是使用模型攻击密钥的能力,该能力使用猜测熵体现。

模型训练的验证精度定义为

$$acc(D_{\text{test}}) = \frac{\mid \{e_i \in D_{\text{test}}\} \mid K^* = \arg\max_k \Pr(K \mid e_i) \mid}{\mid D_{\text{test}} \mid} \quad (2)$$

其中 D_{test} 表示验证集能迹,e_i 表示能迹,K^* 表示正确密钥,$\Pr(k \mid e_i)$ 表示猜测密钥。验证精度就是当猜测密钥和正确密钥相等时的能迹数与验证集能迹数之比。

使用模型进行密钥攻击的猜测熵定义为

$$ge = \mid K \in \kappa \mid p(K) > P(K^*) \mid \quad (3)$$

其中 $p(K)$ 表示猜测密钥的得分,$p(K^*)$ 表示正确密钥的得分。

2 适用于侧信道攻击中卷积神经网络结构设计实验研究

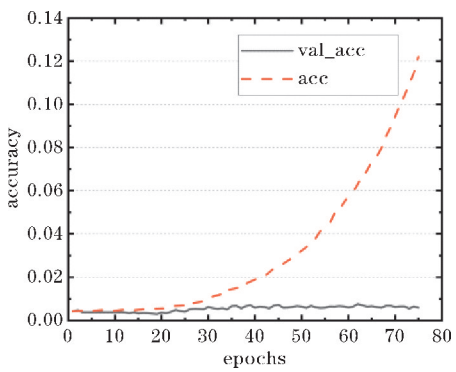
2.1 动机

文献[14]公开了一组具有不同程度抖动防御的侧信道数据集 ASCAD。该数据集是 AES 加掩算法实现的一种电磁信号泄露数据。选择了信息泄露最弱的无掩的 SBOX 输出作为侧信道攻击的目标,对最佳的多层感知器和卷积神经网络结构进行了系统的实验研究。其采用的方法是通过实验对比逐一发现神经网络超参数的最佳值,例如卷积神经网络的网络层数、卷积核大小、激活函数、池化方法,以及网络的训练参数,包括学习率、优化器、训练批大小等。在每一个超参数寻优的实验研究中,其余超参数均保存不变(未优化的超参数采用其设置的默认值,已优化的超参数采用优化实验得到的最佳值)。此外,卷积神经网络的初始结构参照了在图像识别中著名的卷积网络结构 VGG16。

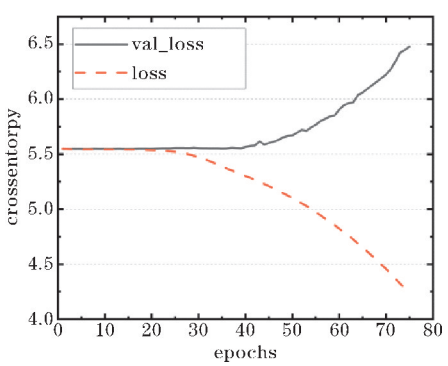
然而遗憾的是,文中探索最佳网络结构的方法从原理上是不正确的。神经网络超参数之所以难以寻找,是因为超参数的最佳值会受到其他超参数设置值的影响,不存在独立的最佳超参数。如果要真正找到最佳的超参数组合,需要对所有超参数的组合进行遍历实验(即网格寻优)。由于超参数很多,其组合更多。这种遍历实验在成本上基本是不可行的。由于采用了不正确的寻优方案,文献[14]得到的“最佳卷积神经网络结构”(文中称为 CNN-best)并不是最佳的。事实上,根据实验研究,依据几项简单的原则设计的卷积神经网络便可以轻易地超过其 CNN-best 的训练和攻击效果。

文献[14]的 CNN-best 结构是:五层的卷积神经网络结构,每一层的 filter 分别为 64,128,256,512,512,卷积核的大小都是 11,每一层采用 relu 激活函数和平均池化函数。该结构所包含的参数非常多。在卷积神经网络中,网络的参数越多,越容易参数过拟合。所谓过拟合是指网络模型对识别训练数据非常有效,但泛

化能力差,识别验证数据能力很差。表现为,随着训练的进行,训练集的精度持续上升、损失持续下降,而验证集的精度和损失则呈现出相反的趋势。其训练超参数受此影响,采用了非常小的学习率(1e-5)和很小的训练批(每批 32 条能迹)。这是因为小的学习率使过拟合的发生变得比较缓慢,模型劣化速度变慢。而使用小批训练是深度学习中的一项防止过拟合的行之有效的经验。然而在极低信噪比的能迹数据训练中,这一经验并不适用。这是因为数据中特征非常微弱,其模型空间中优化方向本身就难以发现。如果使用非常小的训练批,在每次训练中由于数据量太少,更加难以找到正确的梯度优化方向。由于以上这些因素,CNN-best 的训练精度非常差。



(a)训练集精度和验证集精度变化

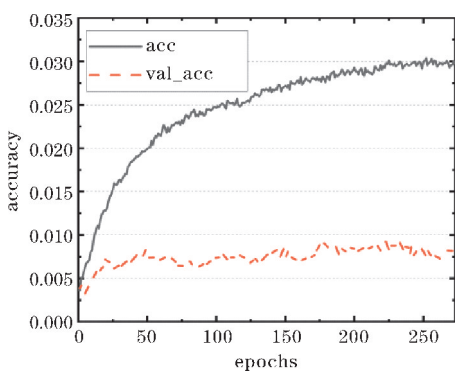


(b)训练集交叉熵损失和验证集交叉熵损失变化

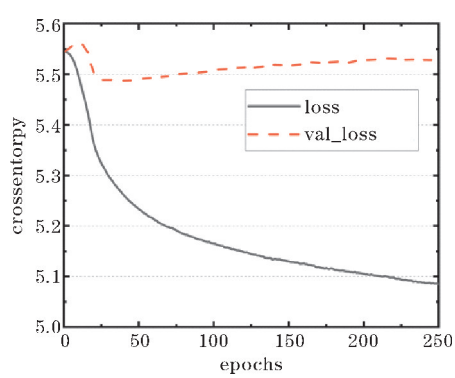
图 2　CNN-best 结构训练结果

研究中重现了 CNN-best 的训练过程。图 2 是 CNN-best 对无抖动防御的加密能耗数据的训练过程。图 2(a)表现了训练过程中训练集精度(acc)和验证集精度(val_acc)的变化。图 2(b)表现了训练过程中训练集交叉熵损失(loss)和验证集交叉熵损失(val_loss)的变化。从图 2 可以看出,随着训练的进行,在训练集精度显著提升的同时,验证精度几乎没有改善;在训练集损失显著下降的同时,验证集的损失在训练前期没有明显降低,且在训练后期出现大幅上升。这是非常典型的过拟合现象,说明模型仅对训练集有效,而对验证集无效。换句话说就是模型的泛化能力很差,这预示了模型在侧信道攻击中不可能有好的表现。在对无抖动防御的数据(desync0)的实验中,最高验证集精度仅达到0.76%,最小验证损失为5.546751。同时,尽管其训练参数采用了非常小的学习率和小训练批,其训练过程仍然出现了严重的过拟合。其过拟合最明显的表现是训练集的损失(loss)和验证集的损失(val_loss)的对比。验证集损失在训练后期大幅上升。

作为对比,实验设计了一个具有 4 层卷积层,3 个平均池化层和一个全连接隐层、一个输出层的神经网络。该网络参数数量只有 CNN-best 的 80%。训练结果如图 3 所示。从图 3(a)可以看出,验证集精度(val_acc)与训练集精度(acc)同步上升,这表现了模型训练是有效的。从图 3(b)可以看出,验证损失在训练前期出现下降后,在训练后期也出现了小幅上升。这表示模型仍然有轻微的过拟合,但情况并不严重。从具体指标来看,实验的最大验证精度达到0.929%,明显高于 CNN-best 的0.76%。最小验证损失5.486637,明显低于 CNN-best 的5.546751。



(a)验证集精度和训练集精度变化



(b)验证集交叉熵损失和训练集交叉熵损失变化

图 3　4 层卷积层训练结果

重现 CNN-best 的实验中,在不同攻击能迹数量下的平均猜测熵(文献[14]中称为“平均排名”:mean rank)与文献中的数据并不一致。这是因为文中攻击

实验中的平均排名只是一次攻击中正确密钥的位置，并不是其声称的平均排名。一次攻击得到的结果偶然性很大。实验中采用 50 次攻击中排名的平均值作为猜测熵，这样才能较为准确地反映出模型的质量。图 4 比较了使用 CNN-best 模型进行 1 次攻击的猜测熵和 50 次攻击的平均猜测熵与攻击能迹数的关系。从图 4 中可以看出，50 次的猜测熵变化比 1 次的要平滑得多，表明其偶然性较小，数值更可靠；同时 CNN-best 的真实攻击效果比文献[14]中表现出来的要差很多。

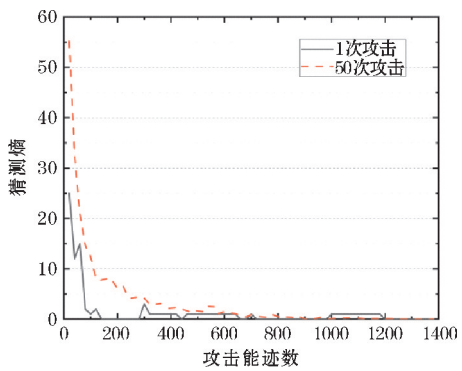


图 4 猜测熵对比

在深度学习的领域中，网络结构的设计更像是一门艺术，需要依靠大量的实践经验，需要设计人员根据其经验总结出一些原则，进而指导其网络结构的优化设计。卷积神经网络起源于图像识别领域，其目前最大的应用领域也仍然是图像识别。在图像识别中积累的经验并不完全适合侧信道领域中对能迹的识别。这是因为图像特征一般是相当明显的（至少对人而言可以一眼识别），而侧信道数据中的有效特征仅表现为能耗随操作数据值的极小幅度的波动，对人而言，完全无法识别。也就是说，侧信道数据的信噪比远比图像的信噪比低很多。因此，对侧信道数据建模的卷积神经网络也需要大量实践经验来指导。因此，根据侧信道能迹的特点，提出了一组设计卷积神经网络的原则，并在实验中证实了这些原则的有效性。

2.2 实验数据

实验采用的是公开的 ASCAD 能迹集以及公开的 DPA Contest V4（DPAV4）能迹集。在 ASCAD 能迹集中包含了 3 种不同的能迹，ASCAD 表示的是同步没有抖动的能迹数据，ASCAD_desync50 表示有 50 个样本抖动的能迹数据，ASCAD_desync100 表示有 100 个样本抖动的能迹数据。每种能迹数据都有 60000 条数据，其中 50000 条作为训练数据，10000 条作为攻击能迹。DPA Contest V4 提供了获取的 10 万条 AES-256 算法的能迹，由于 DPAV4 的信息泄露很明显（信噪比较高），实验中仅采用其中 3 万条能迹作为训练集，1 万条能迹作为攻击测试集。

选择 ASCAD 和 DPAV4 两组实验数据是因为它们的信息泄露程度有很大差异，从而可以总结出基于信息泄露程度的一些网络结构设计原则。信息泄露程度用信噪比（SNR）来表达。信噪比（SNR）是指按中间值对能迹进行分组后，各分组均值的方差与整体方差的均值之比。信噪比计算公式为

$$Var[E[Lt \mid Z]]/E[Var[Lt \mid Z]] \qquad (4)$$

其中 Z 表示按中间值对能迹进行的分组。Lt 表示 t 时刻的噪音观察能迹。图 5 是 ASCAD 的无掩 SBOXOUT 的信噪比与 DPAV4 信噪比的对比，横轴表示能迹的样本位置，纵轴表示信噪比。红色和蓝色分别表示 DPAV4 和 ASCAD 在各样本位置上的信噪比。从图 5 可以看出，DPAV4 数据在样本位置 44500 到 45000 的范围中信噪比出现明显尖峰，说明该数据在这些位置上有明显的信息泄露。而 ASCAD 数据在所有位置上都没有明显的尖峰，说明其没有显著的信息泄露。从最大信噪比来看，DPAV4 达到0.52，而 ASCAD 仅为0.005720658。由此看出，DPAV4 的信息泄露远比 ASCAD 明显。

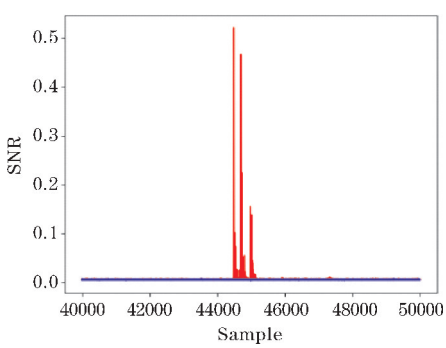


图 5 SNR 对比

2.3 侧信道攻击中卷积神经网络结构设计的经验性原则及其实验验证

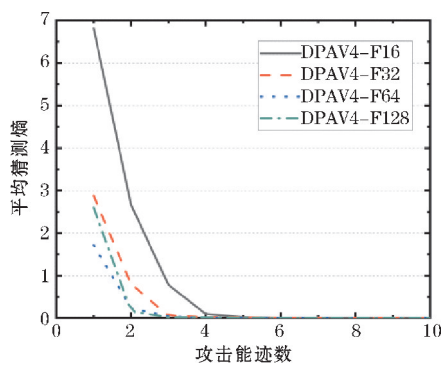
原则 1 能迹的信噪比越低，卷积输出特征应该越小。

卷积输出特征是指在卷积神经网络中通过卷积层和池化层提取得到的特征数量，也就是输入全连接层的特征数量。因为信噪比越低，能耗中包含的特征越少。卷积层能够提取的特征数也应当越少。如果定义的卷积输出特征过多，就很有可能提取到大量的噪音特征。噪音特征过多一方面可能掩盖了有效的泄露信息，从而造成网络无法训练，另一方也可能因噪音特征

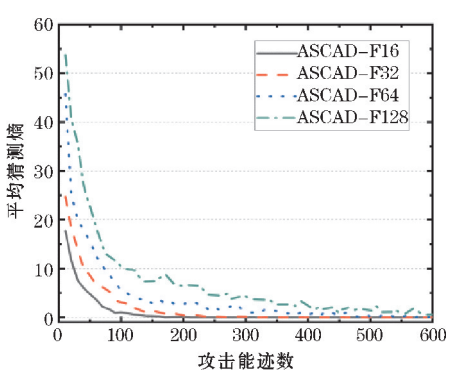
仅对训练集有效,从而导致训练出现严重的过拟合。

为了验证这一原则,对 DPAV4 和 ASCAD 的最佳卷积输出特征数进行了大量实验。实验中,两组数据的卷积神经网络的卷积输出特征数均分别采用 16,32,64,128。对给定的卷积输出特征数,其余超参数采用大量实验进行寻优,最终得到各种输出特征数下的最佳卷积网络结构。实验比较了这些网络在攻击中的效果,用平均猜测熵曲线表示,实验结果如图 6 所示。

图 6 是 DPAV4 和 ASCAD 的不同卷积输出特征数的实验结果。其中,DPAV4-Fn 和 ASCAD-Fn 中的 n 表示卷积输出特征数。从图 6 可以看出,对于 DPAV4,在各种攻击能迹数量的情况下,卷积输出特征 64 的平均猜测熵都是最小的。因此 DPAV4 的最佳的卷积输出特征数是 64;而对于 ASCAD,最佳卷积输出特征数是 16。这是因为 ASCAD 的信噪比明显低于 DPAV4,其能耗数据中包含的有效特征更少,因此卷积输出特征数应当越少。该实验验证了能迹的信噪比越低,卷积层的输出特征应该越小的原则。



(a) DPAV4 不同卷积输出特征数实验结果



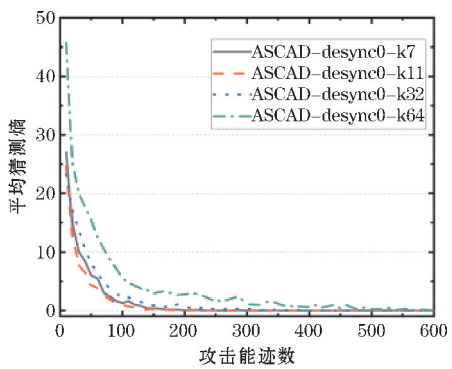
(b) ASCAD 不同卷积输出特征数实验结果

图 6　特征数对比结果

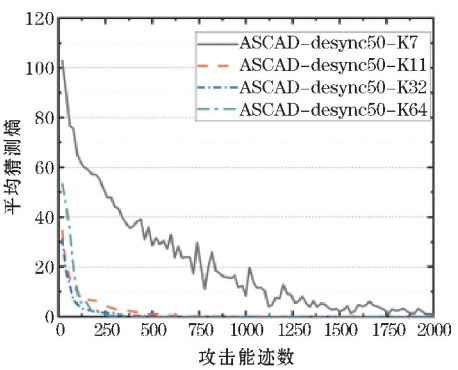
原则 2　能迹中泄露信息越少,首层卷积需要使用更大的卷积核。

首层卷积核的大小决定基本的形状特征。泄露信息越少,能迹形状的差异越小,也就意味着能够提取出的有效特征少。如果卷积核太小就会得不到有效的形状特征,对以后各层提取的特征也会产生影响,这种对特征的提取无效完全可能导致网络无法进行有效学习。

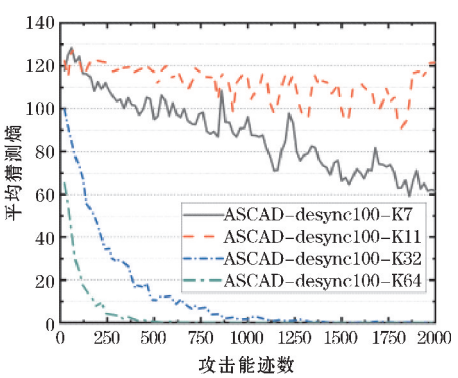
为了验证这一原则,使用 ASCAD 能迹集中的 3 种能迹,分别为 0 抖动、50 个样本抖动和 100 个样本抖动进行了大量实验。数据抖动越严重,信息泄露得越少。3 组数据的卷积神经网络首层卷积核的大小均分别采用 7,11,32,64。对给定了首层卷积核大小,其余的超参数采用大量实验进行寻优,最终得到各种卷积核大小下的最佳网络结构。实验比较了这些网络在攻击中的效果,用平均猜测熵曲线表示,实验结果如图 7 所示。



(a) 无抖动



(b) 50 个样本抖动



(c) 100 个样本抖动

图 7　卷积核大小对模型质量的影响

图 7 是对无抖动、50 个样本抖动和 100 个样本抖动的 3 个能迹集的不同卷积核大小的实验结果。其中

ASCAD-desync*N*-K*n* 中 *N* 表示抖动的样本，*n* 表示首层卷积核的大小。从图 7 可以看出，对于 ASCAD-desync0，在各种攻击能迹数量的情况下，首层卷积核为 11 的平均猜测熵都是最小的。因此 ASCAD-desync0 的最佳首层卷积核大小为 11；对于 ASCAD-desync50，首层卷积核大小为 32 的平均猜测熵最小，而 ASCAD-desync100，首层卷积核大小为 64 的平均猜测熵最小。因为 ASCAD-desync100 泄露的信息相比于 ASCAD-desync0 和 ASCAD-desync50 更少，能迹的形状差异更小，能够提取的有效特征更少，因此首层需要更大的卷积核。该实验验证了能迹中泄露信息越少，首层卷积需要使用更大的卷积核。

原则 3　对能迹建模时，不宜采用过深的卷积网络。

在图像识别中，图像中包含大量特征，以及一些非常抽象的特征，因此需要更深的网络，以便提取非常抽象的特征。而对于侧信道数据是一维能迹数据，没有非常抽象的特征，因此不需要很深的网络。对能迹数据，采用深层的网络进行训练时，特征在前几层就能提取出来。当到后面的层时，有效的特征已经提取完，在进行特征提取已经没有意义。并且实验证明浅层卷积神经网络的训练和攻击效果比深层的卷积神经网络更好，对密钥的安全威胁更大。

为了验证这一原则，采用 ASCAD 能迹集进行了大量实验。改变卷积的深度，通过改变卷积的步长来实现的。采用大于 1 的卷积步长，使卷积层同时起到降维的作用，从而减少卷积的层数。在实验中，3 组数据的卷积步长均分别采用 1，2。对给定了卷积步长，其余超参数采用大量实验进行寻优。当卷积步长为 1 时，卷积网络的结构为 7 层卷积层，卷积步长为 2 时，卷积网络的结构只有 4 层卷积层。实验比较了这些网络的攻击效果，用猜测熵的大小表示，实验结果如图 8 所示。

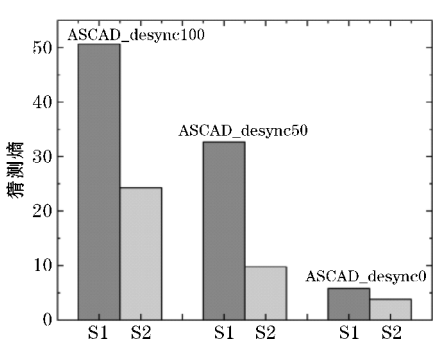


图 8　卷积深度对模型质量的影响

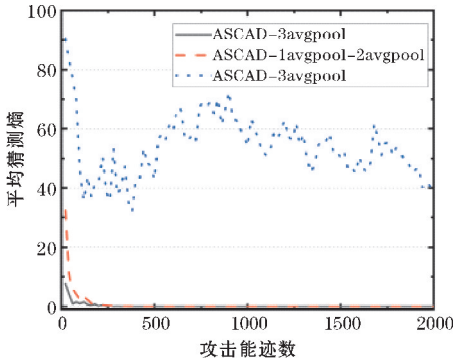
图 8 表示不同数据采用不同卷积深度的实验结果，其中 ASCAD_desync*N* 中的 *N* 表示不同的抖动数，Sn 中的 *n* 表示卷积步长。从图 8 可以看出 3 种数据步长为 2 的猜测熵都要比步长为 1 的猜测熵要小。分析可知，步长为 2 比步长为 1 时，卷积的深度要小，实验结果显示步长为 2 攻击效果更好，因此卷积层不宜过深。该实验验证了对能耗数据建模时，不宜采用过深的卷积层。

原则 4　对抖动严重的能迹，卷积网络中应选择最大池化，而非平均池化。

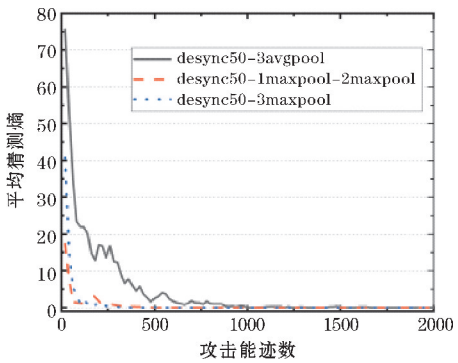
由于抖动，能迹上具有信息泄露的位置没有对齐。不同能迹的信息泄露特征出现在不同的位置上。最大池化可以根据特征的大小，不同能迹从不同位置上选择有效特征，从而在一定程度上达到容忍因抖动而导致的特征错位。而平均池化将一个范围内的多个特征进行平均，虽然也可以起到对抖动的容忍，但由于平均池化将有效特征与无效特征进行了平均，使特征变得不明显。在泄露非常弱的情况下，这种对特征的弱化完全可能导致网络无法进行有效学习。

为了验证这一原则，同样使用了 ASCAD 能迹集对池化函数的选择进行了大量实验。实验中，采用四层卷积层的卷积网络结构，3 组数据的池化函数选择均分别为：都使用平均池化；第一层使用最大池化，后面使用平均池化；都使用最大池化。对给定了卷积使用的池化函数后，其余超参数采用大量实验进行寻优，最终得出使用不同池化函数下的最佳卷积网络结构。实验比较了这些网络下的攻击效果，用平均猜测熵曲线表示，实验结果如图 9 所示。

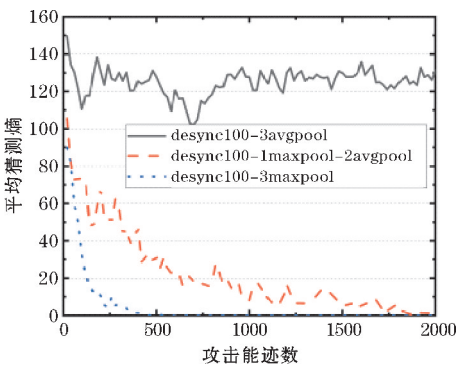
图 9 分别是抖动为 0、抖动为 50 和抖动为 100 的样本在不同池化函数选择下的实验结果。其中 desync*N*–*X* 中的 *N* 表示抖动的样本，*X* 表示选择的池化函数。从图 9 可以看出，对于 desync0，在各种攻击能迹数量的情况下，都采用平均池化的平均猜测熵是最小的。因此 desync0 的池化函数选择应该都使用平均池化函数。对于 desync50，在各种攻击能迹数量的情况下，采用第一层最大池化函数，后面采用平均池化函数的平均猜测熵是最小的。因此 desync50 的池化函数应该选择最大池化函数和平均池化函数的组合。而对于 desync100，都采用最大池化的平均猜测熵是最小的。因为 desync100 相对于 desync50 和 desync0，抖动更严重，泄露的信息更少，采用最大池化能够容忍更多因抖动而导致的特征错位，因此采用最大池化的攻击效果更好。该实验验证了对抖动严重的能迹，卷积网络中应选择最大池化，而非平均池化。



(a)抖动



(b)50 个样本抖动



(c)100 个样抖动

图 9　池化函数选择对模型质量影响

3　结束语

卷积神经网络参数的设定一直较为困难,通过大量的实验研究,总结出侧信道分析中卷积神经网络结构设计的经验性原则,包括信噪比越差,卷积输出特征数应该越小;泄露信息越少,首层卷积需要使用更大的卷积核;对能耗数据不宜采用过深的卷积网络;对抖动严重的能迹,卷积网络中应选择最大池化,而非平均池化。采用这些设计网络结构原则,可以大大提高网络寻优效率。但还有很多超参数需要人工通过大量实验来寻找,因此今后的研究将专注于找出更多的经验。

参考文献:

[1] 杜之波,吴震,王敏,等. 针对 SM4 轮输出的改进型选择明文功耗分析攻击[J]. 通信学报,2015,36(10):85-91.

[2] 吴震,王敏,饶金涛,等. 针对基于 SM3 的 HMAC 的能量分析攻击方法[J]. 通信学报,2016,37(5):38-43.

[3] 杜之波,吴震,王敏,等. 基于 SM3 的动态令牌的能量分析攻击方法[J]. 通信学报,2017,38(3):65-72.

[4] Kocher P C. Timing attacks on implementations of Diffie-Hellman,RSA,DSS,and other systems[C]. Annual International Cryptology Conference,1996.

[5] Kocher P. Introduction to differential power analysis and related attacks[EB/OL]. http://www. cryptography. com/dpa/technical/index. html,1998.

[6] Chari S, Rao J R, Rohatgl P. Template attacks [M]. Cryptographic Hardware and Embedded Systems-CHES 2002. ed:Springer,2003.

[7] Picek, S, Heuser, A, Guilley, S. Template attack versus Bayes classifier[J]. Journal of Cryptographic Engineering,2017(7):343-351.

[8] Bartkewitz,T Lemke-rust K. Efficient template attacks based on probabilistic multi-class support vector machines[J]. Springer,2013:263-276.

[9] Martinasek Z, Hajny J, Malina L. Optimization of power analysis using neural network[C]. International Conference on Smart Card Research and Advanced Applications,2013.

[10] Zdenek Martinasek, Petr Dzurenda, Lukas Malina. Profiling power analysisattack based on MLP in DPA contest V4. 2[C]. In 39th International Conferenceon Telecommunications and Signal Processing. TSP,2016.

[11] Martinasek Z, Hajny J, Malina L. Optimization of power analysis using neural network[C]. International Conference on Smart Card Research and Advanced Applications,Springer Cham,2013:94-107.

[12] Zdenek Martinasek, Lukas Malina, K Trasy. Profiling Power Analysis Attack Based on Multi-layer Perceptron Network[J]. Computational Problems inScience and Engineering,2015(343):317-339.

[13] Eleonora Cagli, Cecile Dumas, Emmanuel Prouff. Convolutional neural networks with data augmentation against jitter-based countermeasures-profiling attacks without pre-processing[C]. In Wieland Fischer and Naofumi Homma, editors, Cryptographic Hardware and Embedded Systems-CHES 2017 – 19th International Conference, Taipei, Taiwan, 2017.

[14] Benadjila R, Prouff E, Strullu R, et al. Study of Deep Learning Techniques for Side-Channel Analysis and Introduction to ASCAD Database[J]. ANSSI, France & CEA, LETI, MINATEC Campus, France, 2018(53).

Experimental Study on the Structure of Convolutional Neural Network Suitable for Side Channel Analysis

HUANG Jie, WANG Yi

(College of Cybersecurity, Chengdu University of Information Technology, Chengdu, 610225 China)

Abstract: In the side channel analysis, the template construct research of template attack has transformed from Gaussian distribution to machine learning algorithm. For example, use support vector machines, neural networks, and so on. However, when using neural networks for side channel analysis, it is difficult to find a suitable network structure due to the large number of design parameters of the network structure. Based on the large number of experimental studies, this paper summarizes and presents the experience of convolutional neural network structure suitable for side channel analysis. It provides a basis for designing the convolutional neural network in the future.

Keywords: side channel analysis; template attack; convolutional neural network