文章编号：2095-4980(2021)04-0717-07

提升能量信息泄漏检测能力的多重 t 检验方案

郑　震，蔡爵嵩，朱春生，郭朋飞，王　恺，严迎建

(信息工程大学 三院，河南 郑州 450001)

摘　要：为应对侧信道能量信息泄漏检测中的多重t检验问题，提出了一种控制多重t检验过程的错误识别率并提升检验效力的泄漏检测方案。在对多重假设检验问题进行分析的基础上引入错误识别率和检验效力作为多重t检验过程中的控制参量。介绍了已有控制多重假设检验问题的方案，结合泄漏检测过程，通过提升检验阈值和调整检验水平的方法对已有控制方案进行了改进，并进行了实验验证。验证结果表明该方案能在提升能量信息泄漏检测能力的同时将检验差错控制在一定范围内。

关键词：侧信道能量信息泄漏；多重 t 检验；错误识别率；检验效力

中图分类号：TP309.7　　**文献标志码：**A　　**doi：**10.11805/TKYDA2019527

Multiple t-test scheme to improve power information leakage detection capability

ZHENG Zhen，CAI Juesong，ZHU Chunsheng，GUO Pengfei，WANG Kai，YAN Yingjian

(The Third Institute, Information Engineering University，Zhengzhou Henan 450001, China)

Abstract：To cope with the multiple t-test issue in the leakage detection of side-channel power information, a leakage detection scheme is proposed to control the false discovery rate of the multiple t-test process and improve the test effectiveness. Based on the analysis of multiple-hypothesis testing issue, the false discovery rate and test effectiveness are introduced as control parameters in the multiple t-test process. Existing schemes for controlling multiple-hypothesis testing issue are introduced. Combined with the leakage detection process, the method of raising threshold and adjusting the test level is proposed to improve the existing control scheme, which is verified by experiments. The verification results show that this scheme can improve the detection capability of power information leakage and control the test errors within a certain range.

Keywords：side-channel power information leakage；multiple t-test；false discovery rate；test effectiveness

在大数据的时代背景下，信息安全领域的攻防技术高速发展，密码攻击手段日益丰富，密码分析设备不断升级，在对密码系统进行安全评估时需要处理的数据量越来越大[1]。利用 t 检验对侧信道能量信息的泄漏进行检测时，为得到全面准确的检验结果，需要进行多次检验，因此在进行检测时会面临多重假设检验问题。一方面，进行检测时对泄漏情况做出决策的依据是一个采集的能量迹样本，因此无法排除得到错误决策的可能性，且单次检验做出错误决策的概率与假设检验的数量成比例地增加[2]，因此在实施包含单个 t 检验数量较多的多重 t 检验时容易对设备的泄漏情况产生误判；另一方面，当代社会需要处理的数据量不断激增，已有文献中控制多重检验问题中错误率的过程检验效力不足的缺陷日益凸显[3]。因此有必要对能量信息泄漏检测中的多重 t 检验问题进行研究，以提高检测能力，减小对泄漏情况做出误判的概率。

1　现有应对多重检验问题的方法

1.1 多重检验问题中的参数

在假设检验问题中，零假设和备择假设的地位并不对等，零假设是受到保护的，因此需要慎重地选择零假

收稿日期：2019-12-06；修回日期：2019-12-23

设[4]。对能量信息进行泄漏检测时，能量迹的众多采样点中能够检测出泄漏的采样点个数较少[5]，且泄漏检测过程中更关注的是存在泄漏的采样点。基于这两点理由，本文将 t 检验的零假设均设置为“H_0：不能在相应的采样点处检测到能量信息的泄漏”。由于零假设是受到保护的，当 H_0 被拒绝时，就有较强的理由确信该采样点处确实存在能量信息泄漏。

一般地，称假设检验中 H_0 为真时拒绝 H_0 的错误为第 I 类错误；H_0 为假时接受 H_0 的错误为第 II 类错误。实际的假设检验问题中通常对犯第 I 类错误的概率进行控制，使其不大于 α，称 α 为显著性水平。为便于对多重 t 检验问题进行讨论，本文引入表 1 中的变量。

表 1　多重 t 检验中的统计量

Table 1 Statistics in multiple t-test

	true null hypothesis	false null hypothesis	sum
refuse	V	S	R
accept	U	T	$m-R$
sum	m_0	$m-m_0$	m

$H_1,H_2,\cdots,H_m$ 为多重 t 检验中的 m 个假设，其中有 m_0 个为正确假设(对应的零假设 H_0 为真)，其余 $m_1(m_1=m-m_0)$ 个为错误假设；R 为 m 次假设检验中被拒绝的假设总数；V 表示在 m 次 t 检验中犯第 I 类错误的次数；T 表示在 m 次假设检验中犯第 II 类错误的次数。此外，S 和 U 分别表示正确地拒绝错误假设和正确地接受正确假设的检验次数。根据各变量的定义可知，在实际中进行 t 检验时，以上各变量中 m 和 R 的值可通过记录得到，其余变量的值则不可观测，只能通过统计的方法对其进行分析。

同时引入检验效力 P 这一参量：

$$P=\frac{S}{m_1}=\frac{S}{m-m_0}=\frac{S}{S+T} \tag{1}$$

检验效力的含义是检验中某控制过程正确地拒绝错误零假设的概率，它表征的是多重检验检测出错误的能力强弱。较高的检验效力表明控制过程的鲁棒性较强，对大样本量的依赖性较小，且检验的效果较好。

目前主要通过控制错误识别率(False Discovery Rate，FDR)来应对多重假设检验问题。控制 FDR 的方法由 Benjamini 和 Hochberg 等提出[6]，FDR 的定义为在多重假设检验中犯第 I 类错误的次数 V 占被拒绝的假设数量 R 的比值的期望。令 $Q=V/R$，则：

$$FDR=\begin{cases}E(Q)=E\left(\dfrac{V}{R}\right), & R\neq 0\\ 0, & R=0\end{cases} \tag{2}$$

FDR 的实际意义较为明确，可以对 FDR 的取值进行调整以适应泄漏检测过程中不同安全级别下的需求[7]。

1.2 针对多重检验问题的控制过程

1.2.1 控制过程中的 p 值法

在单个假设检验中，p 值是由检验统计量的样本观察值得出的零假设可被拒绝的最小显著性水平，是 t 检验拒绝 H_0 时犯第 I 类错误的概率。p 值可以根据检验统计量 t 的样本观察值以及 t 在零假设 H_0 下一个特定的参数值对应的分布函数求出。得到 p 值后，通过将其与显著性水平 α 进行比较即可得出 t 检验的决策：若检验得到的 $p\leqslant\alpha$，则拒绝零假设；若 $p>\alpha$，则接受零假设。

对应于单个假设检验中的 p 值法，在多重假设检验过程中，对错误识别率 FDR，与某检验中假设 H_j 对应的调整 p 值可被定义为：

$$\tilde{p}_j=\inf_{\text{拒绝}H_j}\left\{\alpha\in[0,1]:FDR=\alpha,\text{拒绝}H_j\right\} \tag{3}$$

即假设 H_j 被拒绝时多重检验犯第 I 类错误的总体水平[8]，因此当 $\tilde{p}_j\leqslant\alpha$ 时，拒绝 H_j；$\tilde{p}_j>\alpha$ 时，接受 H_j。通过调整 p 值实质上形成了多重假设检验中的统一标准，便于对各单个检验进行比较分析。

1.2.2 控制错误识别率的多重检验过程

Benjamini 和 Hochberg 首次提出 FDR 的概念，给出了一种控制 FDR 的方法(以下简称 BH 法)，其步骤如下：

1) 分别求出多重假设检验中 m 个假设 $H_1,H_2,\cdots,H_m$ 的调整 p 值 $p_1,p_2,\cdots,p_m$，并按照大小顺序将其排列：$p_{(1)}\leqslant p_{(2)}\leqslant\cdots\leqslant p_{(m)}$；该过程的调整 p 值计算方法：$\tilde{p}_{(j)}=\min_{k=1,2\cdots j}\left\{\min\left(\dfrac{m}{k}p_{(k)},1\right)\right\}$；

2) 从 $p_{(m)}$ 开始依次比较 $p_{(i)}$ 和 $\dfrac{i}{m}\alpha$，找到满足 $p_{(i)}\leqslant\dfrac{i}{m}\alpha$ 的最大的 i，令 $k=\max\left\{i:p_{(i)}\leqslant\dfrac{i}{m}\alpha\right\}$；

3) 拒绝 $H_{(1)},H_{(2)},\cdots,H_{(k)}$，其中 $H_{(i)}$ 为 $p_{(i)}$ 所对应的假设。

可以证明，各假设的检验统计量相互独立时，BH 法可将 FDR 控制在 $\frac{m_0}{m}\alpha$ 以内。

在 BH 法的基础上，Yekutieli 等给出了一种利用重复抽样计算 p 值从而在变量相关的条件下控制 FDR 的方法；Benjamini 和 Liu 等提出了一种“step-down”的控制方法；Hochberg 等提出了一种两阶段的控制方法；Benjamini 和 Hochberg 提出了一种自适应线性向上的控制方法。当前侧信道领域内的攻防技术飞速突破，在对侧信道能量信息泄漏进行检测时，上述各种控制方法检验效力不足的缺陷日益突出。因此需要对现有控制方法进行改进以提升检验效力，适应当前环境下泄漏检测的需求。

2 改进的泄漏检测方案

2.1 改进多重 t 检验检测泄漏过程的方法

本文结合上节中控制 FDR 的基本方法和思想，基于以下思路提出适用于侧信道能量信息泄漏检测的多重 t 检验过程。

1) 提高控制过程中的阈值

BH 法通过依次比较 $p_{(k)}$ 和 $\frac{k}{m}\alpha$，找到满足 $p_{(k)}\leqslant\frac{k}{m}\alpha$ 的最大的 k 来确定需要拒绝的假设。本文对 BH 法中阈值 $\frac{k}{m}\alpha$ 进行调整，将其增大到 $1-(1-\alpha)^{\frac{k}{m}}$。这样，基于不等式 $1-(1-\alpha)^{\frac{k}{m}}>\frac{k}{m}\alpha\quad(1\leqslant k<m)$，增大阈值后的检验过程将拒绝更多假设，从而达到提升检验效力的目的。图 1 是控制过程的示意图。

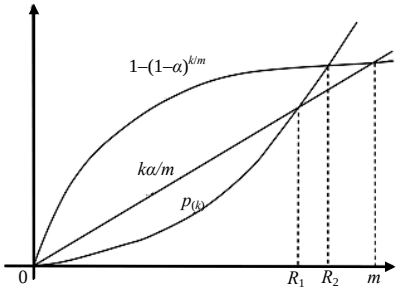

Fig.1 Control process after raising thresholds
图 1 提升阈值后控制过程示意图

图 1 中，$\frac{k}{m}\alpha$ 和 $1-(1-\alpha)^{\frac{k}{m}}$ 所对应的分别是调整前后的阈值曲线，$p_{(k)}$ 对应的曲线表示各假设的 p 值。BH 法的控制过程就是将落在阈值曲线 $\frac{k}{m}\alpha$ 下方的 p 值所对应的所有假设拒绝，即拒绝序号从 0 到 R 的假设；而接受在阈值线上方的 p 值所对应的所有假设，即接受序号大于 R 的所有假设；增大阈值后的比较过程同样拒绝落在阈值曲线下的 p 值所对应的假设，区别在于二者的阈值曲线的轨迹不同。分析图 1 可知，增大阈值前，被拒绝的假设数量为 R_1，增大阈值后，被拒绝的假设数量为 R_2，$R_1\leqslant R_2$。

2) 估计正确零假设占比 π_0，并调整检验水平 α

确定多重假设检验中对正确假设占总假设个数的比例 π_0，并以此为系数调整检验水平 α 能够有效降低检验中的错误率，提高检验效力[9]。目前估计 π_0 的方法主要有：最低斜率估计、蒙特卡罗抽样估计[10]、减密度估计、贝叶斯估计[11]、直方图估计和 λ 估计等。在对各种方法进行分析比较的基础上，本文结合主成分分析(Principle Component Analysis，PCA)对能量迹的降维，提出一种针对能量信息泄漏检测中多重 t 检验的估计真实假设占比 π_0 的方法。

PCA 降维是对原始的 m 维数据进行映射，重新构造形成全新的 n 维特征数据的过程，形成的新特征维度称为主成分。利用 PCA 进行降维时，首先从原始的数据空间中找到一组相互正交的坐标轴，该坐标轴的选择与原始的数据特征相关：第一个新坐标轴选择原始数据中方差(差异性)最大的方向；第二个新坐标轴选择与第一个坐标轴正交的平面中原始数据方差最大的方向，以后的每个新坐标轴均选择与前面的坐标轴正交的平面中方差最大的方向。依此类推，可以得到 m 个新的坐标轴，可以发现，原始数据的大部分差异性包含在前面的 n 个坐标轴中，后面的坐标轴所含方差接近于 0。只保留前面 n 个包含几乎全部方差的坐标轴而忽略后面的 $m–n$ 个坐标轴，最后进行特征提取完成降维。一个变量所含有的信息量可以由其方差衡量，因此降维中这样的取舍实质上是将原始数据中所包含的绝大部分信息分解到前面 n 个方向上，而舍弃掉其余方向上剩余不多的信息量。

本文利用 PCA 对能量迹进行降维，以达到优化检验过程的目的。降维时需要依据式(4)对降维的维数 n 进行确定：

$$\frac{\frac{1}{m}\sum_{i=1}^{m}\|x^{(i)}-x_{\text{app}}^{(i)}\|^2}{\frac{1}{m}\sum_{i=1}^{m}\|x^{(i)}\|^2}\leqslant\varepsilon \tag{4}$$

式中：$x_{\text{app}}^{(i)}$ 为映射值；ε 为进行能量信息泄漏检测时根据所需的不同安全级别设置的值，ε 实质上代表了降维时舍弃掉的信息量在总信息量中的占比，如当 ε=0.05 时，代表降维后保留了原始数据 95%的信息量。将不同的 n 值代入，选取能够满足上式的最小 n 值即为降维后的维数。

一方面，t 检验得到了某采样点处在所需的安全级别下能够检测出泄漏的概率大小，PCA 降维的意义在于降维后维数较少的数据能够包含能量迹中原始功耗数据的绝大部分信息。事实上，能量迹中的所有采样点均存在能量信息的泄漏，只是实际中在一定的阈值设置下泄漏的信息不一定能被检测到。可以近似地认为降维后含信息量较大的一部分采样点为能够检测出能量信息泄漏的点。另一方面，把零假设设置为“H_0：该采样点处不能检测出能量信息泄漏”时，对采集到的能量迹而言，多重 t 检验中 H_0 为真的数目实际上对应的是在所需安全级别下能量迹中不能检测出泄漏的采样点的数目。因此，通过 PCA 降维法可以近似地确定多重 t 检验中真实零假设的占比 π_0：

设采集到的能量迹中采样点的总个数为 n，在一定阈值下根据 PCA 降维得到的能量迹的维数为 n_1，降维过程中舍弃掉的采样点个数为 $n_0\left(n_0=n-n_1\right)$。对能量迹进行 PCA 降维后，可以得到 π_0 的估计值：

$$\pi_0=\frac{m_0}{m}=\frac{n_0}{n} \tag{5}$$

得到 π_0 的估计值后，对检验水平进行调整：

$$\alpha^*=\frac{\alpha}{\pi_0} \tag{6}$$

2.2 改进的泄漏检测方案

综合以上改进方法，本文提出改进的检测过程如下：

1) 采集能量迹，对原始功耗数据进行处理，在相应能量迹采样点处设置零假设。分别求出各假设 $H_1,H_2,\cdots,H_m$ 对应的调整 p 值 $p_1,p_2,\cdots,p_m$，并按照大小顺序将其排列：$p_{(1)}\leqslant p_{(2)}\leqslant\cdots\leqslant p_{(m)}$；

2) 按照 PCA 降维法对原始功耗数据进行降维，估计真实假设占比 π_0，调整检验的显著水平至 $\alpha^*=\frac{\alpha}{\pi_0}$；

3) 将每次比较的阈值设为 $1-\left(1-\alpha^*\right)^{\frac{k}{m}}$，按照基础 BH 过程进行检验，对采样点处的泄漏情况进行判定。

3　方案验证

3.1 验证方法

本文以高级加密标准(Advanced Encryption，AES)算法为例，根据上小节分析将每个采样点处的零假设设置为：“H_0：该采样点处不能检测出能量信息泄漏”，对提出的控制多重 t 检验过程中错误识别率 FDR 的改进方案进行验证。

采集功耗数据时对每条 AES 算法的能量迹设置了 1 250 个采样点。为得到准确、全面、可靠的结论，对每个采样点处的泄漏情况进行 t 检验。因此多重 t 检验中有 1 250 个单独的假设检验。验证过程中需要解决以下几个关键问题。

3.1.1 检验中 p 值的求解

对多重 t 检验中的调整 p 值求解时，需要首先对每个采样点处的单独假设检验的 p 值进行求解。对能量迹中的每个采样点而言，其功耗值服从某正态分布 $N\left(\mu,\sigma^2\right)$。而能量迹中的每个采样点都对应着 AES 算法加密过程中的某中间状态，关于确定“在某采样点处能否检测出能量泄漏”的问题实际上可以转化为“是否能够发现能量迹该采样点处的功耗值与该采样点所对应的 AES 算法的中间状态的数值的相关性”。

检验过程中可以编程对算法的中间状态进行确定，选择得到的中间状态的某一比特，根据该比特的值将采集的能量迹分为两组。求得该比特的值为 0 所对应的分组内功耗的均值，记为 μ_0。记该比特的值为 1 所对应的分组内功耗的均值为 μ_1。这样，对每个采样点处的单独假设检验的 p 值进行求解的过程就转化为了对某正态总体 $N\left(\mu,\sigma^2\right)$，求检验“$H_0:\mu_1=\mu_0;H_1:\mu_1\neq\mu_0$”的 p 值的问题。在该检验问题中，当 $\mu_1=\mu_0$ 时，有 $t\sim t\left(n-1\right)$。在对正态总体 $N\left(\mu,\sigma^2\right)$ 的均值的检验中，当 σ 未知时，可采用统计量：

$$t=\frac{\overline{X}-\mu_0}{S/\sqrt{n}} \tag{7}$$

式中：μ_0 为已求得的中间比特的值为 0 所对应的分组内功耗的均值；$\overline{X}$,S 和 n 分别为中间比特值为 1 所对应的分组内功耗均值的样本观察值、功耗标准差的样本观察值和该组的样本量。设求得的统计量 t 的观察值为 t_0，可参照图 2 对 p 值进行求解。

由图 2 可知，当 $t_0>0$ 时，

$$p=P_{\mu_0}\{|t|\geqslant t_0\}=P_{\mu_0}\{(t\leqslant -t_0)\cup(t\geqslant t_0)\}=2\times(t_0\text{右侧尾部面积}) \tag{8}$$

当 $t_0<0$ 时，

$$p=P_{\mu_0}\{|t|\geqslant -t_0\}=P_{\mu_0}\{(t\leqslant t_0)\cup(t\geqslant -t_0)\}=2\times(t_0\text{左侧尾部面积}) \tag{9}$$

对以上 2 种情况进行综合可知，$p=2\times(t_0$界定的尾部面积$)$。而后可以由得到的 t_0 的值结合 t 函数的分布函数确定采样点处的单独假设检验的 p 值。由于本文所提出的控制方案是基于 BH 法得到的改进方案，因此确定原始 p 值后，可以参考 BH 过程中调整 p 值的方法根据式(10)得到多重 t 检验中的调整 p 值：

$$\overline{p}_{(j)}=\min_{k=1,2,\cdots,j}\left\{\min\left(\frac{m}{k}p_{(k)},1\right)\right\} \tag{10}$$

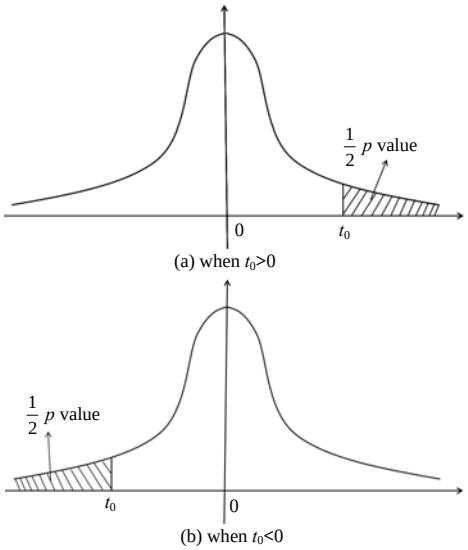

Fig.2 Control process after raising thresholds

图 2 提升阈值后控制过程示意

3.1.2PCA 降维法对正确假设占比的估计

采集 30 000 条 AES 算法的能量迹，按照前文的步骤利用 PCA 进行降维，分析结果如图 3 所示。

图 3 中，横坐标代表能量迹中的各个采样点；纵坐标为各采样点的主成分相关系数，该系数的绝对值越大，相应采样点处所包含的信息量越大，造成能量信息泄漏的可能性也越大。同时可以得到降维后的剩余信息量和降维维数的关系如图 4 所示。

图 4 中，纵坐标代表剩余信息量，取值为 1–ε；横坐标为降维后能量迹中的剩余维数。本文在验证时将 ε 设置为 0.1，根据图 4 可知，此时降维后能量迹中的维数为 120，已知能量迹中的采样点个数为 1 250，由此可进一步估算检测 AES 算法能量信息泄漏的多重 t 检验中真实假设占比 π_0 的值约为 1–(120/1 250)=0.904。

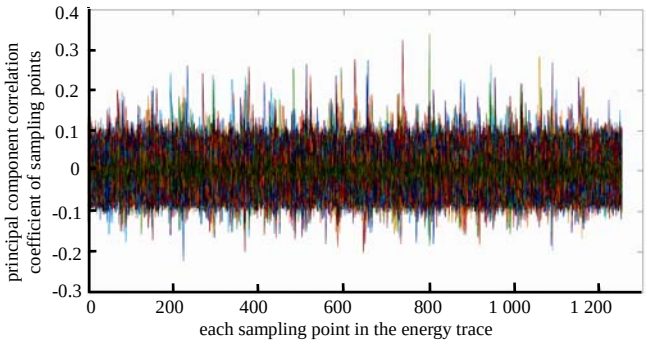

Fig.3 Schematic of PCA dimension reduction

图 3 PCA 降维分析示意图

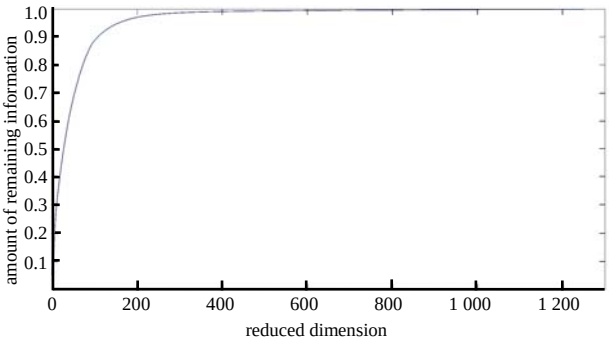

Fig.4 Relationship between the amount of remaining information and the reduced dimension

图 4 剩余信息量与降维维数关系图

对降维后的结果进行逆映射可得到降维前这些关键的特征维度所对应的能量迹中采样点的位置，并据此确定在各个采样点处检验结果的正确与否，并进一步确定多重 t 检验中的错误拒绝数 V、正确拒绝数 S、总拒绝数 R、错误识别率 FDR 和检验效力 P 等参量的值。最后对 FDR 和检验效力进行模拟估计。以错误拒绝数 V 和总拒绝数 R 的比值作为错误识别率的估计值 FDR^*：

$$FDR^*=\frac{V}{R} \tag{11}$$

以正确拒绝数 S 和错误假设的数目 m_1 的比值作为检验效力的估计值 P^*：

$$P^*=\frac{S}{m_1} \tag{12}$$

需要说明的是，FDR^* 是为验证本文提出的控制 FDR 方法的效果而设置的近似值，并非错误识别率 FDR 的确切值。通过近似值的对比，可以在减小验证过程工作量的同时直观地把握本文所提出方案的控制效果。

3.2 实验结果与分析

本节设计如下 3 个对比实验对提出的方案进行评估：

1) 实施 2 次本文提出的改进的控制过程，其中对正确假设占比 π_0 进行估计时分别利用 PCA 降维法和 λ 估计法。最后通过对比 2 次控制过程最终的 FDR 和检验功效对 PCA 降维确定正确假设占比的方法进行评估，得到表 2 中的控制结果。

表 2 PCA 降维与 λ 估计法对比结果

Table2 Results of the comparison of PCA and λ estimation

estimation method	error rejections V	correct rejections S	total rejections R	FDR^*	P^*
PCA	25	58	83	0.31	0.66
λ-estimation	22	55	77	0.29	0.63

分析表 2 可知，相较于 λ 估计法，基于 PCA 降维的估计方法会使得控制过程的错误识别率稍有上升，但可以将检验效力提升到一个更高水平。

分析可知在基于 PCA 降维的估计方法中，阈值设置的不同会导致各项参数的估计值有一定变化，可以通过调整 PCA 降维阈值的方法进一步对方案进行改进，以达到更好的控制效果。

2) 实施 2 次 BH 控制过程，分别将比较的阈值设置为 $\frac{k}{m}\alpha$ 和 $1-(1-\alpha)^{\frac{k}{m}}$，最后比较 2 次控制过程的 FDR 和检验功效，以此对增大阈值的方法进行评估，得到表 3 中的控制结果。

表 3 不同阈值对比结果

Table3 Results of the comparison of different thresholds

thresholds	error rejections V	correct rejections S	total rejections R	FDR^*	P^*
$k\alpha/m$	19	50	69	0.27	0.57
$1-(1-\alpha)^{k/m}$	21	53	74	0.28	0.60

分析表 3 可知，提升阈值后的控制过程能够将错误识别率控制在与提升阈值前相似的水平，并且在一定程度上达到了提升检验功效的控制效果。

3) 分别实施完整的 BH 过程和本文提出的控制过程，对比两个过程最终的 FDR 和检验效力，对本文提出的改进方案的控制效果进行评估，得到表 4 中的结果。

表 4 两种控制方法对比结果

Table4 Results of the comparison of different control methods

control methods	error rejections V	correct rejections S	total rejections R	FDR^*	P^*
BH method	19	50	69	0.27	0.57
improved method	25	58	83	0.31	0.66

与 BH 法相比较，本文提出的方案将错误识别率控制在可接受范围内的同时显著地提升了检验效力。在实际的能量信息泄漏检测中，在将错误识别率控制在一定水平内的前提下，往往不对错误识别率提出更高要求而对检验效力提升的期望较为迫切。根据以上实验过程及其结果分析，本文提出的控制检测泄漏的多重 t 检验中差错率的方法简单易行，一定程度上克服了传统控制方法检验效力不足的问题，具有一定的实际意义。

4　结论

本文对检测侧信道能量信息泄漏的多重 t 检验问题进行了研究，从增大阈值，估计真实假设占比，调整显著水平三方面对已有控制方案进行改进，提出了一种针对能量信息泄漏检测的多重 t 检验问题的改进方案，验证结果表明该方案能在控制错误识别率 FDR 的同时提升检验效力。

后期可进一步研究利用 PCA 降维对真实假设占比进行估计的方法，以提升估计的准确性和可靠性；同时可以考虑将本文提出的改进过程推广应用到其他领域的检验中。

参考文献：

[1] 蔺友江. 概率论教学中的四大公式及其应用[J]. 求知导刊, 2019(6):24-26. (LIN Youjiang. Four major formulas in the teaching of probability theory and their applications[J]. Guidance for Knowledge, 2019(6):24-26.) doi:10.3969/j.issn.

2095-624X.2019.06.009.

[2] LIU Taikang,LI Yongmei. Electromagnetic information leakage testing[M]. Beijing:National Defense Industry Press, 2019. doi:10.1007/978-981-10-4352-9_8.

[3] 王志福,潘旭,金姝,等. 假设检验的原理及其应用[J]. 渤海大学学报(自然科学版), 2013(2):101-105. (WANG Zhifu, PAN Xu,JIN Shu,et al. Principles and applications of hypothesis testing[J]. Journal of Bohai University(Natural Science Edition), 2013(2):101-105.)

[4] MONODEEP K,ARVIND S,SANU K,et al. Reducing power side-channel information leakage of aes engines using fully integrated inductive voltage regulator[J]. IEEE Journal of Solid-State Circuits, 2018(99):1-16. doi:10.1109/JSSC.2018.2822691.

[5] BENJAMINI Y,HOCHBERG Y. Controlling the false discovery rate:a practical and powerful approach to multiple testing[J]. Journal of the Royal Statistical Society Series B(Methodological), 1995,57(1):289-300. doi:10.1111/j.2517-6161.1995.tb02031.x.

[6] BENJAMINI Y,HOCHBERG Y. On the adaptive control of the false discovery rate in multiple testing with independent statistics[J]. Journal of Educational and Behavioral Statistics, 2000,25(1):60-83. doi:10.3102/10769986025001060.

[7] HU Chao,BYENG D,WANG Pingfeng. Fundamentals of probability theory[M]. Berlin,Germany:Springer, 2019. doi:10.1007/978-3-642-28528-8_2.

[8] ZHANG Han,GUO Yuanbo,LI Tao. Multifeature named entity discovery in information security based on adversarial learning[J]. Security and Communication Networks, 2019(2):1-9. doi:10.1155/2019/6417407.

[9] TORSTEN A Enßlin. Information theory:information theory for fields(Ann.Phys.3/2019)[J]. Annalen der Physik, 2019, 531(3):1970017. doi:10.1002/andp.201970017.

[10] 杨会杰,王巍,刘伯栋,等. 典型战术 Ad Hoc 电台一维组网连通性仿真与分析[J]. 太赫兹科学与电子信息学报, 2019,17(3):424-429. (YANG Huijie,WANG Wei,LIU Bodong,et al. Simulation and analysis of the connectivity of a typical tactical Ad Hoc radio one-dimensional network[J]. Journal of Terahertz Science and Electronic Information Technology, 2019,17(3):424-429.)

[11] 许述文,王乐,曾威良,等. 逆伽马纹理复合高斯杂波参数的贝叶斯估计方法[J]. 太赫兹科学与电子信息学报, 2019, 17(4):583-588. (XU Shuwen,WANG Le,ZENG Weiliang,et al. Bayesian estimation of inverse gamma texture compound Gaussian clutter parameters[J]. Journal of Terahertz Science and Electronic Information Technology, 2019,17(4):583-588.)

作者简介：

郑 震(1996-)，男，黑龙江省佳木斯市人，博士，主要研究方向为侧信道安全防护. email:1633019381@qq.com.

朱春生(1988-)，男，河北省邢台市人，博士，讲师，主要研究方向为侧信道安全防护.

王 恺(1992-)，男，太原市人，在读硕士研究生，主要研究方向为侧信道安全防护.

蔡爵嵩(1996-)，男，四川省绵阳市人，在读硕士研究生，主要研究方向为侧信道安全防护.

郭朋飞(1987-)，男，郑州市人，博士，讲师，主要研究方向为 SOC 安全防护.

严迎建(1973-)，男，河南省周口市人，博士生导师,教授,主要研究方向为侧信道安全防护与 SOC 安全防护.