**洋葱路由 VS美国国家安全局**

Nicky van Rijsbergenand Kevin Valk

Radboud University Nijmegen (s4062833)

[n.vanrijsbergen@student.ru.nl](mailto:n.vanrijsbergen@student.ru.nl)

Radboud University Nijmegen (s3052273)

[evin@kevinvalk.nl](mailto:evin@kevinvalk.nl)

**摘要：**

政府和强大组织的数字间谍已经被隐私倡导者警告了许多年了。然而，被美国国家安全局泄露项目的规模还是相当可怕的，即便是专家的项目。

Edward Snowden告诉我们，美国国家安全局正积极地收集尽可能多的信息，并且用任何可能的方法来实现这个目标。他们确实这么做了，例如，努力地影响各种公司的实现和标准来确保后门和弱点会存在。在被Snowden揭露之后，许多人寻求一种方法来保护隐私。然而，鉴于最近发生的事，我们又能相信什么工具呢？

在本文中我们研究了匿名工具洋葱路由。我们观察了对抗NSA这样强大的对手，洋葱路由能提供多少隐私。我们观察了洋葱路由的可用攻击以及NSA能如何使用这些攻击。我们也调查了NSA暴力破解洋葱路由的密码的可能性。为了找到答案，我们假设了NSA有多么强大，并给出了确定的假设。

关键字：TOR,AES,RSA,ECC,NSA

1. **介绍**

在理想的情况下，每个人能决定他们是否希望自己的隐私被泄露。在这种情况下，人们至少应该意识任何侵犯他们隐私的情况，并能随时制止这些侵犯。每个人能控制自己的隐私，并能信任任何人及他人的隐私。这种情况是理想的，因为隐私是每个人的权利，更重要的是，隐私对于所有人来说都是重要的。

不幸的是，现实不是这样理想的情况。由于揭发者Edward Snowden，NSA正以许多人们没想到的方法来从公民身上搜集情报的事已越发明了。起初，人们没意识到这是一种隐私侵犯。但现在，他们明白了，他们试图夺回一部分他们的隐私，但经常不知道该去怎么做。其中一个原因就是因为不清楚NSA的能力。一个许多人试图夺回隐私的方法是用匿名工具；举个例子来说就是洋葱路由，它有超过三百万的用户，是最多被使用的匿名工具。

为了让现实与理想状况更像相似，我们研究了对抗NSA这样强大的对手，洋葱路由是否能够提供隐私。我们提出了以下的问题：对抗NSA洋葱路由能提供怎样程度的保护？

为了得到这个问题的答案，我们首先研究了NSA。NSA已显露的能力是什么（他们已经做了什么）以及NSA预期的能力（他们还可能做什么）。被Edward Snowden揭露的事提供了很大的帮助。我们调查了NSA能做什么来对抗洋葱路由。NSA可以用两种方法来攻击洋葱路由的用户，一是有针对性的，主要是当他们有理由去怀疑某个人，二是通过群众监督，当NSA只是想收集信息。我们已经研究了洋葱路由存在的几个NSA能有针对性性攻击利用的漏洞。我们也观察了洋葱路由的密码系统是否有能力承受得住NSA的攻击。

本文如下组织。第2段给出洋葱路由的介绍。第3段给出对于NSA的全球性看法，以及解释NSA为什么被看作一个敌人。第4段会描述目前已知的对于洋葱路由的攻击，本段也会给出一个关于洋葱路由使用的密码的看法，以及一份这些密码的安全性的详细分析。第5段会总结本文。

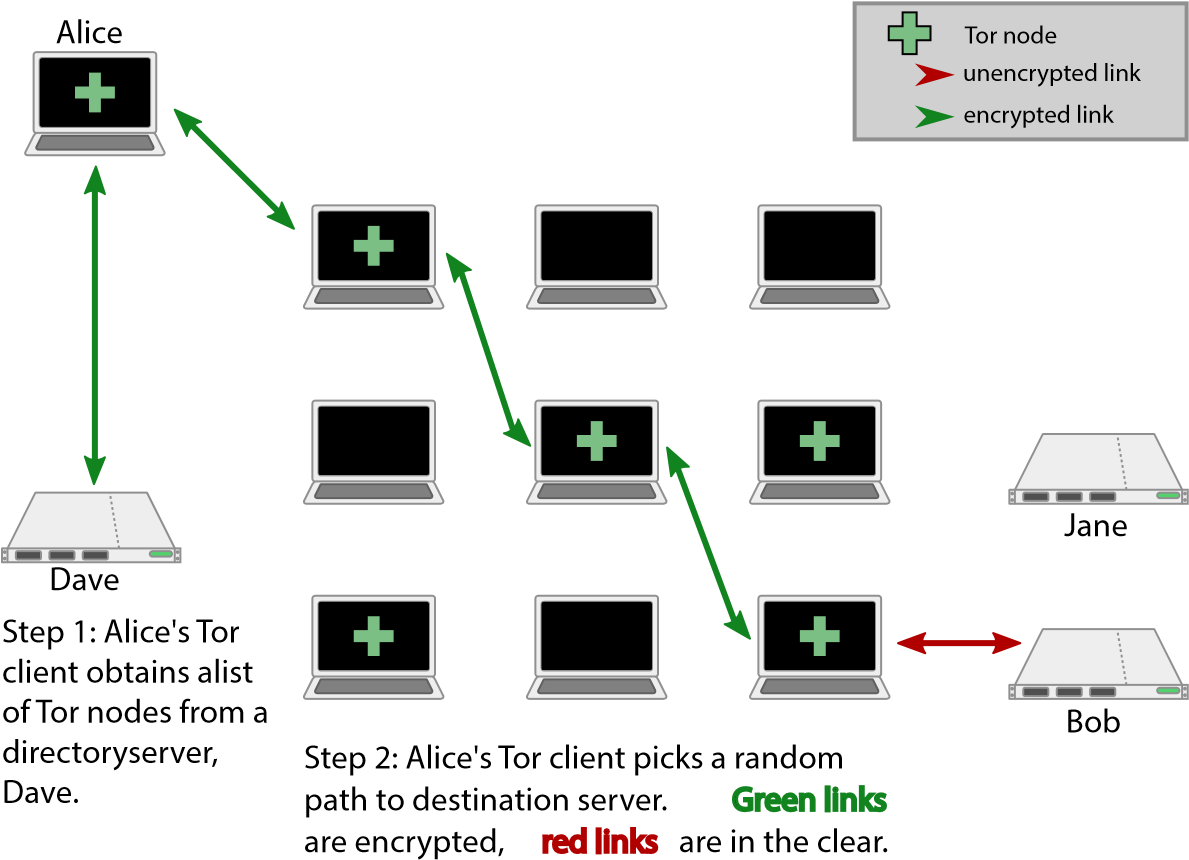
1. **洋葱路由**

洋葱路由是一个开源软件，可以在使用互联网时保持匿名。洋葱路由最初是作为海军研究实验室第三代洋葱路由项目被设计、实施和部署的。记者、军人、政治活动家、举报者、罪犯和普通人现在都可以使用它了。洋葱路由有超过300万的用户。Tor被美国海军研究实验室开发，目前由多家公司和超过4600个个人捐助者赞助。

Tor反弹通过Tor网络的交通来隐藏真正的发送者。外部人员只能看到一个大的Tor网络，但他们并不知道数据包是从哪个网络来的。

* 1. **Tor的全球概述**

Tor通过路由用户通过几个Tor节点（通常是三个）的流量来提供匿名。Tor节点是运行Tor软件的电脑。每个Tor节点都不知道消息的起始点或目的地，或者都不知道。入口节点知道发起者是谁，出口节点知道接受者是谁，中继节点发起者和接受者都不知道。路径的端点（即Tor网络中的发送和结束的点）用X层的加密算法来加密初始的数据包。其中，X相当于路径的长度。这是Tor被叫做洋葱路由的主要原因。因为只有端点知道原始的内容。Tor过去使用RSA加密算法，但是最新版本的Tor使用的是ECC椭圆曲线加密算法。为了提高效率，Tor客户端对发生在每十分钟之内的连接使用相同的路径。之后的请求就会被给予一个新的路径，为的是防止敌人把你早期的操作连接到一个新的路径上。



图一：Tor的概述(来自Justin Findlay(2013)[16]）

Tor也让用户在提供各种服务的同时能够隐藏他们的位置，例如web的发布或者一个即时消息服务器。

**·对于Tor攻击的景象**

Tor只专注于保护数据的传输，所以基本上防止了让外部人员知道他在与谁交谈。Tor不能 提供完全的隐私。当一个对象使用发送包含身份验证的消息，却不使用端到端的加密软件时，Tor仍然会显示关于这个对象的信息。

Tor最近发布了0.2.4版本，它使用了256位的ECC加密算法作为标准，而不是老版本中的RSA-1024算法。原因是因为RSA-1024算法已经不再被认为是安全的了。然而，不是所有Tor客户都更新到最新的版本了，这意味着这些Tor的老客户端可能是脆弱的。

其他针对于Tor的攻击也是存在的。例如，用于关联两个已知的端点的流量/时序分析攻击。坏苹果攻击是另外一个例子，这些例子使用会显示用户信息（例如公共IP地址以及Tor将一个用户的所有流放在同一个电路上的事实）的不安全应用程序。最终，如果敌人控制了N个节点，那么他就可以关联（M/N）2的流量。

1. **国家安全局**

美国国家安全局是美国信号和情报的中央生产者和管理者。据估计，NSA是人事和预算方面美国最大的情报机构之一。对于NSA能够做什么和它已经做了什么有很多的猜测。

由于Edward Snowden，我们不再需要将我们的信息基于关于NSA的谣言。Edward Snowden目前为止大约已经泄露了来自NSA的50~200万份秘密文件，不仅如此，以后还会有更多。这些文件描述了NSA做过的许多间谍活动。这些间谍活动的一部分例子如下：

* 通过影响标准来获得大量数据
* 接受能帮助NSA的所有公司的互联网流量副本，例如AT&T
* 使用大规模监控设备来检测互联网流量
* 对法国、英国、墨西哥等友好国家进行间谍
* 窃听35个世界领导人
* 通过PRISM访问Google和Yahoo的数据库

这些只是NSA到目前为止被揭露了的间谍活动的一部分，许多这些活动违背了欧洲隐私权规定

举报人Edward Snowden唤醒了我们，并让我们意识到了NSA正把矛头指向公民和盟友们，这意味着NSA是我们应该注意的对手。

另外一个NSA应该被看做Tor的敌人的原因，是NSA把Tor看做是一个最高优先的目标。这从Edward Snowden泄露的最高机密幻灯片中可以清晰地看出。这些幻灯片描述了NSA是怎样计划攻击Tor的。

·NSA的黑色预算

NSA不用改被认为只是一个对手，由于他们巨大的黑色预算，更是一个非常强大的对手。他们2013年的黑色预算估计有108亿美元。黑色预算是一个国家用来分配给机密和其他秘密操作使用的。总额中大约有56亿用于数据收集，数据处理和开发以及分析。此外，估计总额中的10亿美元投资在了密码分析和开发。

NSA另一项主要的支出是2013年建立完成的一个大型的数据中心。这个数据中心被叫做“犹他数据中心”，但也被称为“智能社区综合国家网络安全倡议数据中心”。这个数据中心大约100万平方英尺，并且能给NSA 3到12EB的存储容量。

这个数据中心的主要目标当然是未知的，可能是用来存储和处理大量数据。由于Edward Snowden，对于这个数据是什么我们有一个笼统的概念。

1. **Tor vs NSA**

在本节中，我们将会看一看在文献中描述的几次对于Tor的攻击。我们也会看一看NSA怎样才能使用这些攻击来废弃Tor提供的匿名化。最后我们将会分析Tor使用什么样的密码，以及这些密码当前被认为有多强。

* 1. **攻击Tor**

Tor有一些未解决的弱点，我们将在接下来的小章节总结最紧迫的问题。

* + 1. **已知端点的流量分析**

如果两个端点都已知，则会进行流量分析攻击。如果敌人正观察Tor路径的两个端点，那么他介意知道双方是否在跟对方交谈。这意味着如果敌人正在观察Alice（或者路径中的第一跳）和Bob（或路径中的最后一跳），那么这个敌人通过利用统计可以知道Alice和Bob是否正在交谈。例如，敌人可以简单地对Alice发送给Tor网络的数据包进行计数，以及Bob从Tor网络接收到了多少数据包。敌人也可以跟踪Alice发送消息的时间和Bob在什么时候接收到的（又称作时间分析攻击），在一段时间后，敌人将会知道Alice和Bob是都在交谈。开始监控流量的好地方是互联网交换，因为有很多Tor电路只使用一个。

如果对手实际上控制着入口和出口的节点，那么他可以发起一个标记攻击。这基本上意味着他标记了进入Tor网络的数据，并试图找到曾经到达了被他所控制的出口节点的标记。已经被测试过的标记攻击的一个例子，是在Tor使用计数器模式AES的协议级别。敌人可以用正常计数器中断的方法来改变消息。只要信息到达了出口节点，出口节点将会出现解密问题，因为计数器已经不再是正确的了。如果敌人控制着出口节点，他将会注意到这一点。

然而，标记攻击对于敌人来说也是有风险的，因为这会使敌人被注意到的几率更高，这是因为他在数据流中进行了实际的改动，而被动的数据分析则不会。另外，标记攻击被认为是不那么有效的，例如定时攻击。定时攻击的结果导致怀疑这两个人是不是正在与对方交流，这是经常会有的情况。换句话来说，定时攻击几乎没有误报。

NSA可以使用这种攻击，但是他们将会手动地进行，假设NSA没有控制任何Tor的节点。他们需要怀疑这两个人是否真的是在与对方交谈，并且这个攻击将会验证这两个人是否真的在与对方交谈。

* + 1. **坏苹果攻击**

如果一个用户想做一些匿名的事，那他可以使用Tor。然而，如果这个用户在使用Tor的同时使用一些不安全的应用，那他的会话可能受到损害。这是利用Tor的设计和坏苹果攻击来实现的。用这种攻击，可以知道谁在使用不安全的应用。

坏苹果攻击包含两个步骤：

1. 利用用户机器上不安全的应用来显示源IP地址，或者跟踪Tor用户。BitTorrent就是这样一个可用于开始此攻击的不安全应用。使用BitTorrent的Tor用户可以用他的公共IP/端口来建立P2P连接以提高效率，从而不受阻碍地发送他的公共IP/端口。
2. 利用Tor来关联用户的IP地址和安全应用程序的用法。一但对手知道了BitTorrent用户的IP地址，那将很容易显示同一电路中流的IP地址。如果Tor多路复用来自同一电路中一个用户的所有传输时，对手可以将所有这些流与相同的IP地址关联。

显示不同电路中的流的IP地址有点困难，但是这也是可以做到的。BitTorrent创建一个对等的标识符，这个标识符对于每个用户来说都是唯一的。如果对手在不同电路中发现了这个对等的标识符，那么他可以知道这些电路拥有相同的源。当对等体之间的通信被加密时会出现问题。在这种情况下，如果对等体启动了和包含在不同电路中追踪器响应的IP/端口，那么对手可以连接两个电路。

Tor不对第一部分的攻击负责，因为Tor不提供对抗应用层攻击的保护。然而，第二部分的攻击是针对Tor的。

使用这种方法，这种攻击的研究者有能力在只控制了6个退出节点的同时，在23天之内显示出10000个IP地址。这意味着NSA和他们巨大的预算，是有能力识别几乎所有BitTorrent用户的IP地址，因为他们可以做出很多Tor退出节点。

* + 1. **每个电路和分析的节点数量**

敌人控制N个节点中的M个节点可以关联通信中至少（M/N）2的节点。然而，敌人可以吸引更多流量到他M个节点中的一个，从而关联更高数量的流量。Tor使用入口守卫来对抗这种方法，这意味着Tor客户端有一个小的中继节点列表，客户端将会使用这些作为入口节点。如果敌人没有控制这些入口节点中的任何一个，那么控制任何一个用户的通信都是不可能的。如果敌人已经控制了入口节点中的一个，那么他可以关联跟没有设置入口守卫时一样多的通信。因此，如果敌人控制了这些节点中的一个，用户仍然易于分析，但是因为用户仅使用一些节点作为入口节点，敌人现在将会有a((n-c/n))个机会来避免分析，其中C是敌人可以控制或者观察的继电器数量。

一个减少敌人可以做分析的数量的方法是增加每个电路中节点的数量。如果（m/n）2中的n变得更大，你将需要一个更大的m以及拥有相同数量的通信相关量。然而，增加电路的大小也将降低Tor网络的性能，并且因此导致Tor用户的数量减少。更少的用户就会导致更少的流量，并且为了在匿名系统中拥有强匿名性，你需要大量的流量。

这不仅是性能和匿名性之间的权衡，也是大量流量的匿名性和更长路径的匿名性之间的权衡。这种权衡很大方面取决于多少Tor节点预期被破坏。这不包括受攻击的节点总数，而是被某个公司或者一起工作来关联Tor网络上的流量的团队控制的节点总数。

另一个关于Tor的有趣事实是，它允许用户选择他们信任的入口和出口节点。所以，如果用户发现了敌人，那么他可以选择一些他确信不会被攻击的入口和出口节点。

NSA可以很好的利用这种攻击、他们将需要获取许多的Tor节点，来确保他们能经常控制电路中两个或者更多的节点。这将需要钱，但这也是NSA拥有的东西。然而，控制这么多节点将会引起怀疑。

* 1. **加密**
     1. **Tor中使用的加密技术**

Tor源代码是开源的，这让分析Tor中使用的加密函数成为可能的。在表1中，给出了源代码中使用的所有加密函数的摘要（2013年11月13获取）。

|  |  |
| --- | --- |
| **crypto.c** | **aes.c** |
| DH key | EVP when possible |
| RSA | AES CTR (EVP aes ctr128) |
| DER (enc/decode)  ASN.1 (enc/decode) | **General** |
| PKCS1 padding (signature) | TLSv2 |
| SHA1 (signature)  SHA256  HMAC-SHA-256 base32 (enc/decode) (RFC 4648) base64 (enc/decode)  RFC2440 iterated-salted S2K curve25519  3DES (unused) | SSL3 |

表1：源代码中使用的加密函数

**协议**

在本节中，我们将分析什么时候会使用上述命名的加密方案。

在我们深入研究这个协议之前，注意每个Tor节点有三个密钥是很重要的：

用来建立TLS连接的连接密钥

用来加密或者解密加密层的洋葱密钥

用来签名文件和证书的身份密钥

协议的第一部分是在两个节点之间或者一个节点一个客户端之间建立连接。Tor的所有实现都必须支持SSLv3并且应该支持TLSv2。为了建立连接，需要使用TLS握手，在此期间，双方将会在是用什么密码套件上达成一致。一旦双方都在密码套件上达成一致，认证部分将会启动，双方都将使用SHA256和SHA256-HMAC算法。

协议的第二部分是创建一个电路。在这个部分中，SHA-1算法在一个节点的身份密钥来确认完整性。目前有两种握手算法可以使用。Ntor是最新的握手算法，默认在最新版本的Tor中使用。TAP算法默认在所有旧版本的Tor中使用。Ntor算法使用了256位的ECC算法，TAP使用了RSA1024来交换密钥。

协议的第三部分是基于在第二部分中交换的密钥来创建会话密钥。一旦两个客户端都创建了他们的会话密钥，他们就可以通过使用AES128算法安全地进行通信。当电路已经存在了足够长，当前版本的Tor设定为十分钟，它就会被关闭。

* + 1. **Tor中使用的密码安全性**

**·AES**

高级加密标准，正如它的名字所暗示的那样，是国家标准与技术研究所（NIST）在2001年公布的加密标准。AES用三种不同长度大小的密钥来运行：128位、192位、256位。

许多研究人员试图攻破AES但是至今还没有人因为任何明显、实际的攻击而成功。所以我们可以假设唯一可以解密数据的方法就是暴力破解。表2显示了一个对于给定的密钥大小有多少个可能的密钥的近似值。

|  |  |  |
| --- | --- | --- |
| **密钥大小** | **密钥数量** | **攻击之前的平均密钥** |
| 128-bit (AES) | ≈ 3*.*4 · 1038 | ≈ 1*.*7 · 1038 |
| 192-bit (AES) | ≈ 6*.*2 · 1057 | ≈ 3*.*1 · 1057 |
| 256-bit (AES) | ≈ 1*.*1 · 1077 | ≈ 5*.*7 · 1076 |

表2：每个AES密钥大小的密钥数量

以上表格说明，暴力破解一个密钥大小为128位的AES加密算法平均将会进行1.7\*10^38次尝试。一个非常快的GPU实现AES，加密每字节需要大约0.17周期，解密大概需要0.19周期。世界上最快的超级计算机，由一个叫NUDT的公司创造，理论最高速度可达54902.4TFlop/s。在这台超级计算机上暴力破解一个密钥大小为128位的16字节块需要大约秒，或者说2.984\*10^14年。因此暴力破解密钥大小为128位的16字节数据看上去是不可能的。

如果我们假设NSA解密的速度可以达到AES实现速度的两倍，那还是需要2.984\*10^14年来解密一个密钥大小为128位的16字节块。

然而，有很多工作可以通过量子计算。L.K.Grover表明，使用量子计算机，他可以在n个步骤搜索一个n大小的表。假设有一种方法可以在最快的GPU的AES实现上实现这点。那意味着AES-128将会被破坏，并且AES-192处在危险区域。表3显示了假设我们拥有完全可工作的量子计算机，暴力破解AES算法每个密钥大小需要的时间的近似值。

|  |  |  |
| --- | --- | --- |
| **Key size** | **Math**  √ | **Number of seconds** |
| 128-bit  192-bit  256-bit |  | ≈ 414  ≈ 2*.*5 · 1012  ≈ 1*.*0 · 1022 |

表3：用量子计算机暴力破解AES所需的时间

总而言之，我们可以说，没有量子计算机，任何人都几乎不可能暴力破解任何大小的AES密钥。Tor使用了128位的AES算法CTR模式，所以如果某人拥有量子计算机，那么假设他们可以在很短的时间内暴力破解数据。然而，没有迹象表明存在完全可操作的量子计算机。

**·ECC**

椭圆曲线密码学就像RSA，是一个公钥密码体制。ECC算法相对于RSA算法来说的有点就是它可以利用更小的密钥来达到相同水平的安全级别。在2002年，ECC算法被暴力破解的最大的长度是109位。我们将近一步观察256位的ECC算法的安全性，因为这是Tor使用的ECC算法的密钥长度。

暴力破解ECC算法最有效的方法是Pollard’s Rho的方法。这个方法有各种各样的优点，其中，完全并行化是最重要的。因此，相较于GNFS方法来暴力破解RSA，这个方法可以用任何计算机来建立攻击。2002年的攻击有104台计算机来攻击，共花了549天。目前在ECC上实现Pollard Rho方法最快集中在131位的ECC算法。这预示着在拥有2.2GHz时钟频率的AMD羿龙9500四核 64位处理器上总共会运行105年。

有了这个信息，我们可以推算出在256位ECC算法上实现的运行时间。攻击的难度将增加（）。将这个数乘以ECC-131所需的年数将会得到256位ECC算法所需的年数。这个结果大约是12745\*10^23年过着1.2745\*10^14亿台计算机用以上所述的处理器运行大约一年。

NIST已经提出了双椭圆曲线确定性随机位发生器（Dual EC DRBG），这个发生器可以由ECC用来产生随机数。Dual EC DRBG拥有比其他已知随机数发生器更高效的方法。与许多密码系统一样，ECC只有在随机数发生器提供足够的随机性时才是安全的。

然而，NSA故意影响标准或者他们自己创造出弱化的标准。他们对Dual EC DRBG这样做，并且这不是一个例外。例如，他们可能创造出一个给对手在寻找“随机”数时使用的有好处的识别器。

总结一下，我们可以说暴力破解256位的ECC算法不是一个好的选择。这意味着一个正确实现的256位ECC算法是安全的。

1. **小结**

由于Edward Snowden的揭发，我们现在更好地了解了什么是NSA。我们了解了他们想收集尽可能多的信息，并且他们拥有106亿美元来实现这个目标。

我们已经看到对于Tor的几种攻击是存在的，并且他们有能力使Tor提供的匿名性无效化。然而，这些攻击仅仅在同一路径的两个目标节点都是NSA拥有，或者Tor网络的大部分都在NSA手中才是可能的。

尽管RSA-1024算法被认为是不安全的，有理由不再使用它。但是，256位的ECC算法和AES-128任然被认为是安全的。然而，不确定是关于NSA的。慢慢地我们得到了更多关于NSA能做什么的信息，但是我们不知道他们是否比学术界更先进。我们也不知道NSA控制了多少Tor节点。

作为最后的结论，我们想说，如果说到大量的监控，假设NSA和学术界一样的先进，Tor将会提供对抗NSA的保护。然而，如果NSA特别针对某个人，那么只使用Tor将不会得到足够多的保护。

**参考文献**

1. G. Acar, M. Juarez, N. Nikiforakis, C. Diaz, S. Gu¨rses, F. Piessens, and B. Preneel. FPDetective: dusting the web for fingerprinters. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, CCS ’13, pages 1129–1140. ACM, November 2013. http://www.cosic.esat.kuleuven.be/publications/ article-2334.pdf.
2. A. Acquisti, R. Dingledine, and P. Syverson. On the Economics of Anonymity. In *Financial Cryptography*, volume 2742 of *Lecture Notes in Computer Science*, pages 84–102. Springer, 2003. http:

//freehaven.net/doc/fc03/econymics.pdf.

1. J. Ball. NSA monitored calls of 35 world leaders after US official handed over contacts, Oktober 2013. http://www.theguardian.com/ world/2013/oct/24/nsa-surveillance-world-leaders-calls.
2. J. Bamford. The NSA Is Building the Country’s Biggest Spy Center (Watch What You Say), March 2012. http://www.wired.com/ threatlevel/2012/03/ff\_nsadatacenter/all/1.
3. S. L. Blond, P. Manils, A. Chaabane, M. A. Kaafar, C. Castelluccia, A. Legout, and W. Dabbous. One Bad Apple Spoils the Bunch: Exploiting P2P Applications to Trace and Profile Tor Users. *USENIX Workshop on Large-Scale Exploits and Emergent Threats*,

4, March 2011. https://www.usenix.org/legacy/events/leet11/ tech/full\_papers/LeBlond.pdf.

1. J. W. Bos, M. E. Kaihara, T. Kleinjung, A. K. Lenstra, and P. L. Montgomery. On the security of 1024-bit rsa and 160bit elliptic curve cryptography. *IACR Cryptology ePrint Archive*,

2009. http://lacal.epfl.ch/files/content/sites/lacal/files/ papers/ecdl2.pdf.

1. J. W. Bos, D. A. Osvik, and D. Stefan. Fast implementations of aes on various platforms. *IACR Cryptology ePrint Archive*, 2009. http://eprint.iacr.org/2009/501.
2. D. R. L. Brown. Conjectured security of the ansi-nist elliptic curve rng. *IACR Cryptology ePrint Archive*, 2006. http://www.math.ntnu. no/~kristiag/drafts/dual-ec-drbg-comments.pdf.
3. Certicom. Certicom Announces Elliptic Curve Cryptosystem (ECC) Challenge Winner, 2002. http://www.certicom.com/2002-pressreleases/340-notre-dame-mathematician-solves-eccp-109encryption-key-problem-issued-in-1997.
4. Council of Europe. European Convention on Human Rights. November 1950. http://echr-online.com/art-8-echr/introduction.
5. J. Daemen and V. Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002. http://www.springer.com/computer/ security+and+cryptology/book/978-3-540-42580-9.
6. G. Danezis. The Traffic Analysis of Continuous-Time Mixes. In *Proceedings of the 4th International Conference on Privacy Enhancing Technologies*, PET ’04, pages 35–50. Springer, 2004. http:

//freehaven.net/anonbib/cache/danezis:pet2004.pdf.

1. R. Dingledine and N. Mathewson. Tor protocol specification. November 2013. https://gitweb.torproject.org/torspec.git/ blob\_plain/ac3824c45dde87849e531e75248e7495e0047028:/torspec.txt.
2. R. Dingledine, N. Mathewson, and P. Syverson. Tor: The SecondGeneration Onion Router. 2004. http://oai.dtic.mil/oai/oai? verb=getRecord&metadataPrefix=html&identifier=ADA465464.
3. EFF. NSA Spying on Americans, 2013. https://www.eff.org/nsaspying.
4. J. Findlay. Tor website PNG diagrams as SVG. November

2013. https://lists.torproject.org/pipermail/tor-dev/2013November/005762.html.

1. X. Fu and Z. Ling. One Cell is Enough to Break Tor’s Anonymity. *Black Hat DC*, 2009. https://www.blackhat.com/presentations/ bh-dc-09/Fu/BlackHat-DC-09-Fu-Break-Tors-Anonymity.pdf.
2. B. Gellman and A. Soltani. NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, October 2013. http://www.washingtonpost.com/world/national-security/nsainfiltrates-links-to-yahoo-google-data-centers-worldwidesnowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74d89d714ca4dd\_story.html.
3. K. Gjøsteen. Comments on dual-ec-drbg/nist sp 800-90 draft december 2005. March 2006. http://www.math.ntnu.no/~kristiag/ drafts/dual-ec-drbg-comments.pdf.
4. D. Goldschlag, M. Reed, and P. Syverson. Onion Routing for Anonymous and Private Internet Connections. *Communications of the ACM*, 42(2):39–41, February 1999. http://www.onion-router.net/ Publications.html#CACM-1999.
5. D. M. Gordon. Discrete Logarithms in *GF*(*P*) Using the Number Field Sieve. *SIAM Journal*, 6:124—-138, 1992. http://www.ccrwest. org/gordon/log.pdf.
6. G. Greenwald. XKeyscore: NSA tool collects ’nearly everything a user does on the internet’. July 2013. http://www.theguardian.

com/world/2013/jul/31/nsa-top-secret-program-online-data.

1. L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219. ACM, 1996. http://arxiv. org/abs/quant-ph/9605043.
2. Guardian. British spy agency taps cables, shares with nsa

-. June 2013. http://www.reuters.com/article/2013/ 06/21/usa-security-britain-idUSL5N0EX39I20130621http: //www.reuters.com/article/2013/06/21/usa-security-britainidUSL5N0EX39I20130621.

1. T. Guardian. ’tor stinks’ presentation. October 2013. http:

//www.theguardian.com/world/interactive/2013/oct/04/torstinks-nsa-presentation-document.

1. M. Hosenball. NSA chief says Snowden leaked up to 200,000 secret documents, November 2013. http://www.reuters.com/article/ 2013/11/14/us-usa-security-nsa-idUSBRE9AD19B20131114.
2. M. R. Jens Glu¨sing, Laura Poitras and H. Stark. Fresh Leak on US Spying: NSA Accessed Mexican President’s Email, October 2013. http://www.spiegel.de/international/world/nsahack-email-account-of-mexican-president-a-928817.html.
3. A. Juels. RSA-768 Factored, January 2010. https://blogs.rsa. com/rsa-768-factored/.
4. J. Larson and J. Elliott. Government standards agency “strongly” discourages use of NSA-influenced algorithm, September 2013. http://arstechnica.com/security/2013/09/governmentstandards-agency-strongly-suggests-dropping-its-ownencryption-standard/.
5. Lunar. Tor Weekly News, September 2013. https:

//blog.torproject.org/blog/tor-weekly-news-%E2%80%94september-11th-2013.

1. D. Matthews. America’s secret intelligence budget, in 11 (nay, 13) charts. August 2013. http://www.washingtonpost.com/blogs/ wonkblog/wp/2013/08/29/your-cheat-sheet-to-americassecret-intelligence-budget/.
2. S. J. Murdoch and P. Zielin´ski. Sampled Traffic Analysis by InternetExchange-Level Adversaries. In *Proceedings of the Seventh Workshop on Privacy Enhancing Technologies*, PET ’07, pages 167–183. Springer, June 2007. http://www.cl.cam.ac.uk/~sjm217/papers/ pet07ixanalysis.pdf.
3. J. L. Nicole Perlroth and S. Shane. Secret Documents Reveal N.S.A. Campaign Against Encryption, September 2013. http:

//www.nytimes.com/interactive/2013/09/05/us/documentsreveal-nsa-campaign-against-encryption.html?\_r=0.

1. NUDT. Tianhe-2 (MilkyWay-2), November 2013. http://www. top500.org/system/177999.
2. L. Øverlier and P. Syverson. Locating Hidden Servers. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, SP ’06, pages 100–114. IEEE Computer Society, May 2006. http://www.onionrouter.net/Publications/locating-hidden-servers.pdf.
3. N. Perlroth. Government Announces Steps to Restore Confidence on Encryption Standards, September 2013. www.nytimes.com/interactive/2013/09/05/us/documentsreveal-nsa-campaign-against-encryption.html?\_r=0.
4. J. Rachels. Why Privacy is Important. *Philosophy & Public Affairs*, 4(4):323–333, 1975. http://www.jstor.org/stable/2265077.
5. O. Schirokauer. Discrete Logarithms and Local Units. *Theory and Applications of Numbers without Large Prime Factors*, 345(1676):409––423, 1993. http://www.jstor.org/stable/54275.
6. A. Shamir and E. Tromer. On the Cost of Factoring RSA-1024. 2729:1–26, 2003. http://link.springer.com/chapter/10.1007% 2F978-3-540-45146-4\_1.
7. A. Solani. NSA influences standards, September 2013. https:// twitter.com/ashk4n/statuses/375725741830598657.
8. Tor. Tor FAQ: Entry guards. November 2013. https://www. torproject.org/docs/faq.html.en#EntryGuards.
9. Tor. Tor metrics portal: Users. December 2013. https://metrics. torproject.org/users.html.
10. Tor. Tor: Sponsors. 2013. https://www.torproject.org/about/ sponsors.html.en.
11. U.S. Navel Research Laboratory. Onion Routing. March 1997. http:

//www.onion-router.net/Archives/onions-1997.txt.

1. S. D. Warren and L. D. Brandeis. The Right to Privacy. *Harvard Law Review*, 4(5):193–220, December 1890. http://www.jstor.org/ stable/1321160.