Computer Science and Application 计算机科学与应用, 2018, 8(1), 59-66
Published Online January 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.81009

Hans汉斯

Analysis of Trojan-Horse Attack against Untrusted Source

Jiatao Yu[1,2], Hongxin Li[1], Wenzu Ge[3], Guilin Zhang[1,3], Yu Han[1], Shuyi Zhang[1], Wei Wang[1]

[1]Strategic Support Force Information Engineering University, Luoyang Henan
[2]PLA No.95833 Force, Beijing
[3]PLA No.68303 Force, Lanzhou Gansu
Email: lihongxin830@163.com

Received: Jan. 3rd, 2018; accepted: Jan. 22nd, 2018; published: Jan. 29th, 2018

Abstract

The rapid development of information age puts forward higher requirements on information security protection. In recent years, quantum cryptography based on the theory of quantum physics gets more and more attention because of its reliability and high efficiency. However, the practical quantum key distribution system often cannot achieve the ideal state, which causes many security problems to the practical communication system. Firstly, this paper introduces the Ekert91 quantum key distribution (QKD) protocol based on quantum entanglement. Then, we propose a partial Trojan-horse attack scheme against this protocol and analyze the theory, process and the effect of the attack. The scheme measures thirty percent of EPR photon pairs used in the formation of security keys, the eavesdropper can obtain twenty-nine point two-five percent of security keys and only causes zero point seven-five percent error rate. The scheme possesses important theoretical significance and realistic feasibility.

Keywords

Quantum Key Distribution, Untrusted Source, Ekert91 Protocol, Trojan-Horse Attack

针对非可信源的特洛伊木马攻击技术研究

于家涛[1,2]，李宏欣[1]，葛文祖[3]，张贵林[1,3]，韩　宇[1]，张书轶[1]，王　伟[1]

[1]战略支援部队信息工程大学，河南 洛阳
[2]解放军95833部队，北京
[3]解放军68303部队，甘肃 兰州
Email: lihongxin830@163.com

收稿日期：2018年1月3日；录用日期：2018年1月22日；发布日期：2018年1月29日

文章引用: 于家涛, 李宏欣, 葛文祖, 张贵林, 韩宇, 张书轶, 王伟. 针对非可信源的特洛伊木马攻击技术研究[J]. 计算机科学与应用, 2018, 8(1): 59-66. DOI: 10.12677/csa.2018.81009

摘　要

飞速发展的信息时代对信息安全保护提出了更高的要求，近年来基于量子物理属性的量子密码因其安全高效的优点而受到广泛关注。然而实际量子密钥分发系统往往达不到理想状态，这给实际通信系统带来很多安全性问题。本文首先介绍了基于量子纠缠的Ekert91量子密钥分发协议的原理和基本流程，在此基础上，借鉴基于极化单光子量子密钥分发协议中的特洛伊木马攻击思想，设计了针对纠缠协议的量子黑客攻击方案，同时对攻击思想、攻击原理、攻击步骤以及攻击效果进行了详细的分析。通过验证分析，所提攻击方案针对构成安全密钥的EPR光子对总量的30%进行测量，窃听者可以获得29.25%的安全密钥且只引入0.75%的误码率，具有重要的理论意义和现实可行性。

关键词

量子密钥分发，非可信源，Ekert91协议，特洛伊木马攻击

1. 引言

量子密码学是量子力学和密码学有机结合的前沿学科，而量子密钥分发(Quantum Key Distribution，简称 QKD)技术作为其主要研究内容，发展最为迅猛，我国自主研发的量子通信卫星将于 8 月份择期发射，其主要用途就是分发密钥和进行量子纠缠实验。QKD 为远距离的通信双方 Alice 和 Bob 之间提供无条件安全的共享密钥，进而利用经典的“一次一密”加密算法来实现无条件安全的量子保密通信[1]。通信双方通过量子信道来传递信息，所谓量子信道就是能够很好地传送单个量子系统且与外界隔离的信道，对保护量子系统具有十分重要的作用。量子物理学，特别是不可克隆原理保证了以下两点内容：1) 合法用户可以检测到量子信道中任何窃听者的存在；2) 合法用户可以确定窃听者通过攻击量子信道所获信息的上限。因此，合法用户可以确定隐私放大在信息保护中的应用下限。

随着量子信息技术的飞速发展，通信双方在量子信道中传递的密钥信息存在被窃取的可能。通常假设窃听者(Eve)具有量子存储功能，可以在量子力学允许的范围内进行窃听和攻击，从而获得密钥信息。显然，Eve 实施的攻击并不局限于量子信道，其可以攻击通信双方的设备(量子物理学不能为保护通信双方设备提供帮助)，也可利用 QKD 实际执行过程中的漏洞来实现攻击。由于实际 QKD 系统所采用的物理器件存在不完美特性，不完全符合理想 QKD 协议的安全性需求，窃听者可以利用这些安全性漏洞来窃取密钥信息。量子力学基本原理为 QKD 系统的理论安全性提供了保证，而 QKD 系统的实际安全性却仍制约着自身的实用化发展。因此挖掘实际 QKD 系统中非理想物理器件所引起的安全性漏洞，对于 QKD 从理论研究向实际应用发展具有十分重要的现实意义。

近年来实际 QKD 系统不断发展和成熟，但实际系统中的安全性漏洞仍是各国研究团队分析与研究的热点问题。在实际双向 QKD 系统中，由于窃听者可以完全控制光源，所以 QKD 光源的光子数分布完全未知，此类光源被称为非可信源。目前针对非可信源的量子黑客攻击主要分为四种：大脉冲攻击、相位重映射攻击、被动法拉第镜攻击、特洛伊木马攻击。本文重点研究针对量子密钥分发协议的特洛伊木马攻击方案。

在实际安全性分析中，特洛伊木马攻击(Trojan Horse Attack，简称 THA)受到了国内外研究机构的重点关注，针对 THA 的分析与研究日趋增多。2008 年北京师范大学的邓富国等人通过两次单光子测量和六次幺正变换提高了多方量子秘密共享协议的安全性[2]，该协议可以抵抗准备量子信号的秘密分享者实施的 THA。同年邓富国等人提出了一种实际双向量子通信协议[3]，利用该协议的鲁棒性可防止窃听者通过 THA 窃取量子信道中的密钥信息，这意味着双向量子通信协议在实际应用过程中也是安全的。2014 年北京工业大学的杨宇光等人提出了基于 BKM07 协议的延迟-光子特洛伊木马攻击[4]，并对 BKM07 协议进行了一些改进，使其能够更好地处理 THA 带来的安全性问题。2014 年青岛理工大学的马鸿洋和范兴奎提出了抵抗 THA 的量子密钥多播通信协议[5]，但目的量子节点的个数是固定的，如何动态处理节点个数仍需要深入研究。2014 年德国埃尔朗根-纽伦堡大学的 Nitin Jain 等人发现特洛伊木马攻击能够对实际量子密码技术的安全性造成威胁，并在 ID Quantique 公司的商业 QKD 系统上成功实现了特洛伊木马攻击[6]。同年 Nitin Jain 等人对实际 QKD 系统中的 THA 进行了风险分析[7]。2015 年内蒙古工业大学的杨秀清等人证明了在实际情况中利用目前的技术手段来攻破部分 QKD 系统是非常容易的[8]，并介绍了两种可用于双向协议的 THA：延迟-光子攻击和隐形光子攻击。2015 年东芝欧洲研究中心的 Lucamarini 等人将 THA 转换为信息泄露问题，这样就可以对系统安全性进行量化并与光学元件的规格联系起来，并在此基础上提出了 QKD 系统中 THA 的实际安全界限[9]。2016 年，信息工程大学马鸿鑫等提出了针对连续变量的特洛伊木马攻击思想，并取得了一定的效果[10]。

以上针对 QKD 协议的特洛伊木马攻击方案均建立在基于极化单光子协议基础之上，针对基于纠缠协议的攻击方案目前文献研究相对较少。本文借鉴特洛伊木马攻击思想，针对最初也是最具代表性的两粒子纠缠态协议 Ekert91 协议[11]进行分析，窃听者通过 THA 获取接收方 Bob 端的测量基信息，然后在通信双方共享安全密钥之后，利用截取-重发的方法对测量基相同的部分 EPR 光子进行测量，进而获取部分安全密钥。所提方案可以获得大部分安全密钥而引入较小的误码率，并能够应用到基于多粒子纠缠的协议中，具有现实可行性和推广价值。

2. Ekert91 协议

1991 年，牛津大学的 Ekert 提出了基于纠缠光子信号的量子保密通信协议，简称为 Ekert91 协议。该协议利用量子纠缠来共享高安全性密钥，同时利用经典通信的方式对密钥进行检验并确定最终用于通信的安全密钥。其中，通过利用 Alice 和 Bob 测量基不同部分的测量结果进行 Bell 不等式的计算，可以检测出 Eve 存在的可能性，进而保证了 Ekert91 协议的安全性。

Ekert91 协议的示意图如图 1 所示：Alice 在本地制备好 EPR 光子对，再将其中一个光子传输给 Bob。这样 Alice 和 Bob 之间就共享一对 EPR 光子。首先，通信双方分别对自己持有的 EPR 光子进行测量并保留测量结果，其中测量基从两个特定基 $\{+,\times\}$ 中随机选取；经过多次测量以后，通信双方在经典公共信道上公布各自随机选取的测量基，保留同时测量成功的部分。如果测量基相同，则保留对应的测量结果；而测量基不同的部分则通过经典公共信道告诉对方；然后，对该部分的测量结果进行 Bell 不等式的计算，根据不等式的破坏程度可检验系统的安全性；最后，在保证系统安全性的情况下，由于量子纠缠导致通信双方的测量结果具有强关联性，所以测量基相同部分对应的测量结果可以作为通信双方共享的安全密钥。

3. 特洛伊木马攻击方案

3.1. 攻击思想

在过去的十年里，各国研究团队陆续发现 QKD 的物理实现过程中的一些漏洞，而这些漏洞的出现主

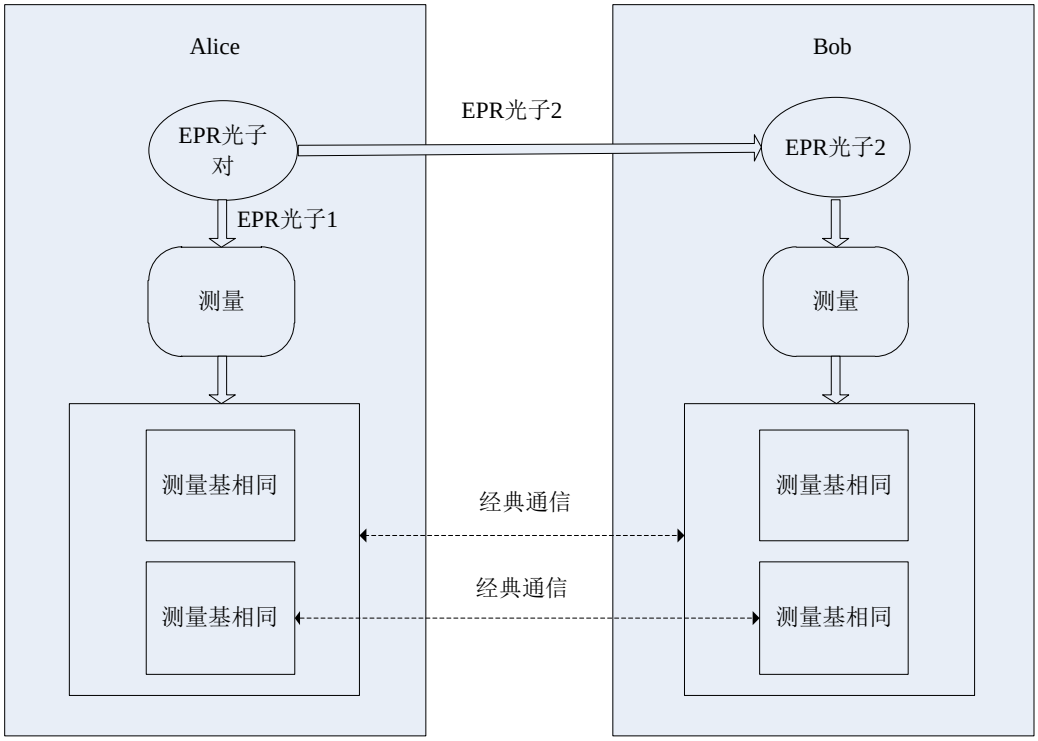

Figure 1. Progress of Ekert91 protocol
图 1. Ekert91 协议示意图

要是由于技术的非理想性或硬件的缺陷。射入 QKD 系统的光脉冲会在某些位置发生 Fresnel 反射和 Rayleigh 散射，导致一些光向输入光信号的反方向传播。因此，一些 QKD 系统内部元件的特性和功能可通过发射强光并分析背向反射光进行研究，这就构成了 THA 的基础。

Eve 占据部分开放的量子信道，使用一个辅助光源发射强光进入 Alice 或 Bob 的系统。由于 QKD 系统中任何光学元件都存在反射光，Eve 可通过分析调制元件(如相位调制器或偏振调制器)的反射光来获取测量基信息，进而利用简单的截取-重发攻击获得密钥信息。这种攻击被称为特洛伊木马攻击。准确的说，THA 利用了量子信道对 Eve 开放的特点，针对的不是 Alice 和 Bob 之间传递的光子，而是 Alice 或 Bob 端的光学元件。尽管存在强度可被 Eve 探测的反射光，但在目前的技术条件下想通过测量反射光来获得 Alice 调制信号的信息仍很难实现。

3.2. 攻击原理

每一种量子保密通信协议的实现方法都有自身的特点，协议的使用范围也各不相同。而本章提出针对 Ekert91 协议的攻击方案，就是为了更加全面地分析 THA 技术，对攻击效率的提高和防御策略的研究有着重要的参考价值。

在通信双方分别对自己持有的 EPR 光子进行测量之前，密钥是无法确定的，因此 Eve 无法在 EPR 光子传输过程中窃取任何信息。在通信双方公布各自随机选取的测量基之前，Eve 无法确定通信双方选取的测量基是否相同，进而无法窃取通信双方共享的安全密钥。如果 Eve 想窃取安全密钥，那么它必须复制并保留一个 EPR 光子且不被通信双方发现，直至通过经典公共信道获取测量基，才能通过测量获取安全密钥。其中，复制 EPR 光子是违背量子不可克隆原理的，同时在现有技术条件下想长期存储量子态也是很难实现的。

本章提出了针对 Ekert91 协议的特洛伊木马部分攻击方案，基本原理是 Eve 通过 THA 获取 Bob 的测量基信息，然后在通信双方共享安全密钥之后，利用截取-重发的方法对测量基相同的部分 EPR 光子进行测量，进而获取部分安全密钥。通常假设 Eve 具有量子存储功能，可以在量子力学允许的范围内进行窃听和攻击。

3.3. 攻击步骤

THA 攻击 Ekert91 量子保密通信协议的具体流程如下，如图 2 所示：

1) 根据参考文献 13 的窃听装置和攻击思想，Eve 可通过 THA 获取 Bob 端 90%的测量基信息。

2) EPR 光子对的共享方式有很多种。假定 Alice 在本地制备好 EPR 光子对后，再将其中一个光子传输给 Bob。通信双方分别对自己持有的 EPR 光子进行测量并保留测量结果，其中测量基从两个特定基 $\{+,\times\}$ 中随机选取。

3) 经过多次测量以后，通信双方在经典公共信道上公布各自随机选取的测量基，保留同时测量成功的部分。

4) 如果测量基相同，则保留对应的测量结果并作为通信双方共享的安全密钥，而测量基不同的部分则通过经典公共信道告诉对方。

5) 通常假设 Eve 具备量子存储能力。Eve 利用截取-重发的方法对 30%用于形成安全密钥的 EPR 光子进行测量，但 Eve 只知道 Bob 端 90%的测量基信息，所以其只能获取部分安全密钥。

3.4. 攻击效果分析

本章所提攻击方案有利于 Eve 获取安全密钥信息，攻击效果分析过程如下：

1) 因为通信双方的测量基都是从 $\{+,\times\}$ 中随机选取的，所以测量基相同的概率为 50%。导致 Alice 传输给 Bob 的 EPR 光子只有一半用于形成通信双方共享的安全密钥。下面讨论 Eve 对所有用于形成安全

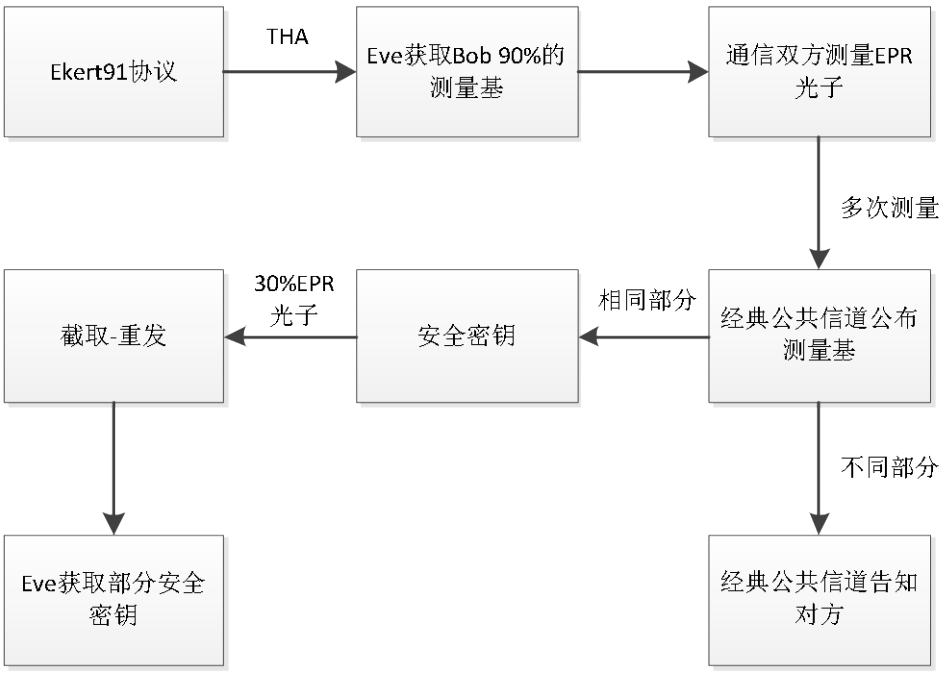

Figure 2. Progress of THA against Ekert91 protocol
图 2. THA 攻击 Ekert91 协议流程图

密钥的 EPR 光子进行测量这种情况。

由表 1 可知，因为 Eve 知道 90%的 Bob 测量基信息，所以 Eve 可通过测量 EPR 光子获取 90%的安全密钥。

2) 对于剩下 10%未知的 Bob 测量基信息，不妨设 Bob 选取+基进行测量。此时，Eve 选取+基或×基进行测量的概率各为 50%。

由表 2 可知，因为 Eve 无法获取剩下 10%的 Bob 测量基信息且选取+基或×基进行测量的概率各为 50%，所以在 Eve 选取+基进行测量时其可以获取 5%的安全密钥，而在选取 × 基进行测量时，虽然不能获取完全正确的安全密钥，但是也有一定概率获取安全密钥。

3) 对于剩下 5%未知的安全密钥，Eve 选取×基进行测量，不妨设 Alice 的测量结果为 1。

由表 3 可知，Eve 选取 × 基对 Alice 传输的测量结果 1 进行测量，测量结果各有 50%的概率为 0 或 1。然后 Bob 利用 + 基对 Eve 传输的测量结果 0 或 1 进行测量，测量结果也各有 50%的概率为 0 或 1。也就是说，Alice 的测量结果 1 在 Eve 的作用下可变为 0、1、0、1，概率各为 25%，即 Eve 可获取 2.5%的安全密钥，剩下 2.5%的安全密钥则无法得知。

因此，在上述这种情况下，Eve 可获取 97.5%的安全密钥，同时引入了 2.5%的误码率。

4) 本章所提攻击方案选取 30%的 EPR 光子进行测量，Eve 可以获得 97.5%×30% = 29.25% 的安全密钥，同时将误码率降到 2.5%×30% = 0.75%，从而进一步降低通信双方发现 Eve 存在的可能性。

正如上文所述，考虑到 EPR 光子在传输过程中存在被窃听的危险[12]，这可能会对 Ekert91 协议共享安全密钥的过程造成干扰，进而引入一定的误码率。为了能够最大程度地降低 Eve 所引起的误码率，我

Table 1. Known 90% of Bob's measurement basis information
表 1. 已知 90%的 Bob 测量基信息

Alice 测量基	测量结果	Eve 接收所用基	接收结果	Eve 发送所用基	发送结果	Bob 测量基	测量结果	对基后是否保留
+	0	+	0	+	0	+	0	是
+	1	+	1	+	1	+	1	是
×	0	×	0	×	0	×	0	是
×	1	×	1	×	1	×	1	是
+	0	×	0 或 1	×	0 或 1	×	0 或 1	否
+	1	×	0 或 1	×	0 或 1	×	0 或 1	否
×	0	+	0 或 1	+	0 或 1	+	0 或 1	否
×	1	+	0 或 1	+	0 或 1	+	0 或 1	否

Table 2. Unknown 10% of Bob's measurement basis information
表 2. Bob 测量基信息的 10%未知

Alice 测量基	测量结果	Eve 接收所用基	接收结果	Eve 发送所用基	发送结果	Bob 测量基	测量结果	对基后是否保留
+	0	+或×	0 或 1	+或×	0 或 1	+	0 或 1	是
+	1	+或×	0 或 1	+或×	0 或 1	+	0 或 1	是
×	0	+或×	0 或 1	+或×	0 或 1	+	0 或 1	否
×	1	+或×	0 或 1	+或×	0 或 1	+	0 或 1	否

Table 3. Eve chooses × basis
表 3. Eve 选取 × 基

Alice 测量基	测量结果	Eve 接收所用基	接收结果	Eve 发送所用基	发送结果	Bob 测量基	测量结果	对基后是否保留
+	0	×	0 或 1	×	0 或 1	+	0 或 1	是
+	1	×	0 或 1	×	0 或 1	+	0 或 1	是
×	0	×	0	×	0	+	0 或 1	否
×	1	×	1	×	1	+	0 或 1	否

们使用低损信道代替原有信道进行 EPR 光子的传输。通过使用低损信道传输 EPR 光子，安全密钥的误码率可被限制在一定范围内，从而不会引起通信双方的注意，Eve 可以继续利用该攻击方案获取安全密钥信息。

4. 结论与展望

近年来，量子保密通信蓬勃发展，而 QKD 系统作为其重点研究方向，逐步从理论研究走向实际应用。由于实际 QKD 系统所用的物理器件存在非完美特性，导致实际系统与理想模型之间存在一定差异，而窃听者通常会利用这些差异来实施量子黑客攻击，进而获取部分或全部密钥信息。

本文主要针对实际 QKD 系统中非可信源问题进行了量子黑客攻击技术的分析与研究。其中，我们提出了一种新的攻击方案：针对 Ekert91 协议的特洛伊木马部分攻击方案。该方案针对构成安全密钥的 EPR 光子对总量的 30%进行测量，Eve 可以获得 29.25%的安全密钥且只引入 0.75%的误码率，同时可使用低损信道代替原有信道以降低所引入误码率的影响。在攻击方案的设计过程中，我们将 EPR 光子对的共享方式假定为 Alice 产生并传输给 Bob。但在 Ekert91 协议中 EPR 光子对的共享方式却有很多种，共享方式的改变可能会影响攻击方案的效率，所以针对 Ekert91 协议的 THA 技术研究还任重而道远。相信随着科技水平的不断提高，实际 QKD 系统中的非完美因素将逐渐减少，THA 技术的研究将进入一个崭新的阶段，这对量子逆向分析技术的发展具有重要的现实意义。

参考文献 (References)

[1] 李宏欣, 李瞻, 闫宝, 韩宇, 王伟, 山灵. 全球量子保密通信技术进展研究[J]. 计算机科学与应用, 2017, 7(1): 74-87.

[2] Deng, F.G., Li, X.H. and Zhou, H.Y. (2005) Improving the Security of Multiparty Quantum Secret Sharing against Trojan-Horse Attack. *Physical Review A*, **72**, 440-450. https://doi.org/10.1103/PhysRevA.72.044302

[3] Deng, F.G., Zhou, P. and Li, X.H. (2005) Robustness of Two-Way Quantum Communication Protocols against Trojan-Horse Attack. http://arxiv.org/abs/quant-ph/0508168

[4] Yang, Y.G., Sun, S.J. and Zhao, Q.Q. (2014) Trojan-Horse Attacks on Quantum Key Distribution with Classical Bob. *Quantum Information Processing*, **14**, 681-686. https://doi.org/10.1007/s11128-014-0872-1

[5] 马鸿洋, 范兴奎. 抗特洛伊木马攻击的量子密钥多播通信协议[J]. 通信学报, 2014, 35(7): 193-198.

[6] Jain, N., Anisimova, E. and Khan, I. (2014) Trojan-Horse Attacks Threaten the Security of Practical Quantum Cryptography. *New Journal of Physics*, **16**, 123030-123051. https://doi.org/10.1088/1367-2630/16/12/123030

[7] Jain, N., Stiller, B. and Khan, I. (2014) Risk Analysis of Trojan-Horse Attacks on Practical Quantum Key Distribution Systems. *IEEE Journal of Selected Topics in Quantum Electronics*, **21**, 168-177. https://doi.org/10.1109/JSTQE.2014.2365585

[8] Yang, X.Q., Wei, K. and Ma, H. (2015) Trojan-Horse Attacks on Counterfactual Quantum Key Distribution. *Physics Letters A*, **380**, 1589-1592. https://doi.org/10.1016/j.physleta.2015.09.027

[9] Lucamarini, M., Choi, I. and Ward, M.B. (2015) Practical Security Bounds against the Trojan-Horse Attack in Quan-

tum Key Distribution. *Physical Review X*, **5**, 1030-1056. https://doi.org/10.1103/PhysRevX.5.031030

[10] Ma, H.X., Bao, W.S., *et al.* (2016) Quantum Hacking of Two-Way Continuous-Variable Quantum Key Distribution Using Trojan-Horse Attack. *Chinese Physics B*, **25**, 080309. https://doi.org/10.1088/1674-1056/25/8/080309

[11] Ekert, A.K. (1991) Quantum Cryptography Based on Bell's Theorem. *Physical Review Letters*, **67**, 661-663. https://doi.org/10.1103/PhysRevLett.67.661

[12] Gisin, N., Ribordy, G., Tittel, W., *et al.* (2002)Quantum Cryptography. *Reviews of Modern Physics*, **74**, 145-195. https://doi.org/10.1103/RevModPhys.74.145