基于模型检测的半量子密码协议的安全性分析

杨 帆[1]，杨国武[1]，郝玉洁[2]

(1. 电子科技大学大数据研究中心 成都 611731；2. 电子科技大学计算机科学与工程学院 成都 611731)

【摘要】对于密码协议而言，安全性是其最核心的关键问题，对于量子密码协议来说也一样。研究人员可以通过各种手段证明这些协议是安全的，但存在极大的困难，因为这对数学功底有着很高的要求。该文利用全自动化的技术——模型检测，采用了形式化验证方法，即基于概率的模型检测工具PRISM，来对半量子密码协议进行建模并验证其安全性。该方法避免了传统基于数学方法验证的繁杂，提高了验证的速度和效率。验证的结果也表明，当传输足够多的光子时，检测出窃听的概率无限趋近于1，和全量子密码协议一样，半量子密码协议也是安全的。

关 键 词 窃听； 模型检测； PRISM； 半量子密码

中图分类号 TP301.2 文献标志码 A doi:10.3969/j.issn.1001-0548.2017.05.013

Security Analysis of Semi-Quantum Cryptography Protocols by Model Checking

YANG Fan[1], YANG Guo-wu[1], and HAO Yu-jie[1]

(1. Big Data Research Center, University of Electronic Science and Technology of China Chengdu 611731;

2. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 611731)

Abstract For cryptography protocols, security is its most core issue, and is the same for quantum cryptography protocols. Researchers can adopt many methods to prove that these protocols are secure, but there exists much difficulty. By using the method of formal verification and the technique of model checking, a fully automated probabilistic model checking tool - PRISM can be used to model these protocols and verify the security properties. Such a methodology can not only avoid the computational complexity of the traditional verification methods based on mathematics, but also improve efficiency and accelerate the verification process. The verification results show that the detection rate of eavesdropping is approximately close to 1 when sufficient photons are transmitted. The semi-quantum cryptography protocols is as secure as the full quantum protocols.

Key words eavesdropping; model checking; PRISM; semi-quantum cryptography

密码学是在第三方(敌手)的存在下，保障安全通信的技术和实践。量子密码学是量子力学和传统密码学结合的产物，依靠微观粒子的量子属性实现对信息的保护。量子密码学研究的主要目标是抵抗量子计算攻击的密码算法和协议，是密码学的一个重要分支。

1 半量子密码协议

现阶段，量子密码协议主要包括量子密钥分发协议(quantum key distribution, QKD)[1-2]、量子秘密共享协议(quantum secret sharing, QSS)[3-5]、量子签名协议(quantum signature, QS)[6-7]、量子安全直接通信协议(quantum secure direct communication, QSDC)等。量子密钥分发协议允许两个合法的用户Alice(A)和Bob(B)生成只有他们知道的密钥来加密和解密信息，即便是在有窃听者Eve(E)监听的情况下。著名的量子密钥分发协议有BB84、B92、SARG04等，这些协议假设A和B都能进行量子操作，如使用不同的测量基来制备和测量光子。

半量子密钥分发协议(semi-quantum key distribution, SQKD)最早是在2007年提出的[8]，后来又有许多新的版量子密钥分发协议被提出[9-15]。SQKD尝试实现相同的目标——生成安全的密钥来抵抗敌手的攻击。与量子密钥分发协议不同的是，半量子密钥分发协议中的一个用户(通常为B)是无法进行量子操作的。

收稿日期：2016－03－21；修回日期：2017－03－06

基金项目：国家自然科学基金(61272175, 61572019, U1230106)

作者简介：杨帆(1985－)，男，博士生，主要从事形式化方法和量子密码协议方面的研究.

一个SQKD协议通常通过如下过程来执行。量子用户A随机选择测量基制备一个量子比特并发送到信道中。该量子比特传输到经典用户B之后，B只能进行如下两种操作之一：

1) B可能测量并重传该量子比特。B只能采用正交基 $Z=\{|0\rangle,|1\rangle\}$ 进行测量，并将结果回传给A。即如果B测量结果是 $|r\rangle(r\in\{0,1\})$，那么B将 $|r\rangle$ 回传给A。

2) B可能直接将量子比特回传给A而不进行任何操作，B不会得知该比特的任何状态信息。

不管B如何选择，量子比特回传到A之后，A可以进行任意操作，如用任意测量基进行测量。

本文对文献[16]提出的半量子密钥分发协议进行详细描述。

本文采用的半量子密钥分发协议是半量子的。半量子是进行通信的双方中，其中一个用户(在本文中假设为B)无法进行量子操作而只能进行经典操作，即B只能够采用测量基Z对量子比特进行测量和回传，或者直接回传。其次，该协议是一个单量子态的协议，即用户A(A为量子用户)在每一个循环中，必须传输一个量子比特状态，且该量子比特状态是单独公开的。

本文协议的量子通信过程的执行步骤如下：

1) 用户 A 制备状态 $|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$，并传入信道中。

2) B选择一个随机值 $k_B\in\{0,1\}$ 作为在本次循环中所使用的候选的初始密钥。

① 假如 $k_B=0$ (此时概率为50%)，那么用户B将会把该量子比特直接回传；

② 假如 $k_B=1$，用户B将会用测量基Z对该量子比特进行测量，并重新制备一个与测量结果相同状态的量子比特并传入信道中。如B用Z测量基进行测量，得到测量结果 $|r\rangle$ (其中 $r\in\{0,1\}$)，然后将 $|r\rangle$ 重传给A，并将测量结果存为 m_B ($m_B=r$)。

3) A 选择测量基 Z 或 X 来进行测量(X 由状态 $|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)$ 构成)。

① 如果A选择X测量基(概率为50%)进行测量，则得到测量结果为 $|-\rangle$，于是把初始密钥设为 $k_A=1$；

② 如果A选择Z测量基(概率依然为50%)进行测量，得到的测量结果为 $|1\rangle$，则初始密钥设为 $k_A=0$；

③ 其他情况下，将初始密钥设为 $k_A=-1$。

将上述过程重复执行N次(N足够大)后，用户A和B会使用公共信道去掉某些循环，该公共信道是经过认证的。首先，用户B会告诉A去掉他测量为 $|1\rangle$ 的循环；其次，用户B会在 $k_B=0$ (直接回传)的循环中随机选择合适的比例并去掉，即使 $k_B=0$ 和 $k_B=1$ 的概率相等；最后，用户A告诉B将 $k_A=-1$ 的循环去掉。

2 模型检测

形式化验证是证明一种实现是否与设计规范完全一致。在现代工业的硬软件系统设计中，特别是在集成电路的设计中，得到了广泛的大规模的应用。形式化验证是在一个系统下，使用数学的形式方法证明或证伪设计算法对于某种形式规范或性质的正确性。实践证明，形式化验证在组合电路、密码协议、以源代码形式表示的软件和具有内部存储器的数字电路等系统的正确性验证中是很有帮助的。

在复杂系统的构建中，花费在验证上的时间和精力远比设计多，所以人们一直在寻求更易实现并扩大覆盖范围的技术。在安全协议的验证方面使用最多的技术就是模型检测[17]。

模型检测是指对一个给定的系统，使用抽象的方法得到一个模型，采用穷尽的方法自动检查该模型与所给定的规范是否相符合。这是一种能够自动验证有限状态系统性能正确性的方法和手段。一类重要的模型检测方法已开发出来，可用于检查硬件和软件设计的模型。这里的规范由时序逻辑公式给出。在模型检测中，时序逻辑公式的开创性工作由文献[18-21]完成。

使用模型检测的方法对密码协议进行安全性验证所采用的基本思路是，建立一个相对小的能运行相关协议的系统模型，以及能与协议交互的入侵者模型[22]。实现模型检测的方法有很多，包括时序逻辑[23]、Büchi自动机[24]和GSTE[25]等。

由于量子现象的过程是随机的，所以使用基于概率随机过程的模型检测是最合适的方法。PRISM就是这样一种概率模型检测器，由伯明翰大学开发。PRISM能构建并分析若干种概率模型，使用得最多的模型包括离散时间马尔可夫链(DTMCs)、连续时间马尔可夫链(CTMCs)、马尔科夫决策过程(MDPs)、概率时间自动机(PTAs)和概率自动机(PAs)等。模型使用PRISM语言描述，是一种简单的、基于状态的语言。

在量子密码协议的验证中，模型检测已经表现出了强大的优势[26-28]。而对于半量子密码协议来说，

现有的方法都是通过数学证明验证其安全性，使用模型检测来对其安全性进行验证几乎没有。本文使用PRISM对文献[16]中的SQKD协议进行验证。

3 半量子密码协议的安全性分析

根据第1节中的叙述，本文使用PRISM语言来重新描述协议。

3.1 协议描述

在PRISM中，将半量子密钥分发协议的执行过程分解为若干模块，每个模块代表系统的一个部分。在本文中，半量子密钥分发协议中的每个部分都有一个模块与其一一对应。同时，单独使用一个模块来表示量子信道。在每个模块中，都有若干操作和仅在该模块中起效的局部变量。

按照协议的执行过程，将其分为用户A模块(即Alice)、用户B模块(即Bob)、信道模块和窃听者模块(即Eve)4个部分。每一个模块又按照执行顺序分为若干个状态。当执行某一个具体的操作时，整个模块的状态就会发生改变。

1) 用户 A(Alice)模块

① 在Alice将光子(量子比特)发送到信道中后，状态由初始状态“0”变为“1”；② Alice得到Bob回传的光子后，状态变为“2”；③ Alice选择测量基，状态由“2”迁移到“3”；④ Alice对光子进行测量，状态变为“4”；⑤ Alice进行错误率的检测。若错误率≥阈值，则检测到Eve，状态变位“5”；⑥ 判断光子传输是否结束。若未完成，返回到“0”；否则，状态变为“6”终止。

具体的过程如图1所示。

2) 用户 B(Bob)模块

初始状态也为“0”，如图 2 所示。

① Bob选择进行何种操作，状态变为“1”；② Bob进行测量，状态变为“2”；③ Bob得到结果，状态变为“3”；④ Bob将光子回传给Alice，状态由“3”迁移到“4”；⑤ 判断传输是否结束。若未完成，状态返回“0”；若完成，变为“5”结束。

3) 信道模块

初始状态为“0”，执行过程如图3所示。

① Alice将光子传输到信道中，模块状态变为“1”；② Eve截获到光子，信道状态由“1”变为“2”；③ Eve将光子重新传到信道中，状态变为“3”；④ Bob从信道中接收到光子，状态迁移到“4”；⑤ Bob将光子回传到信道中，状态由“4”迁移到“5”；⑥ Alice得到光子，信道状态回到初始态“0”。

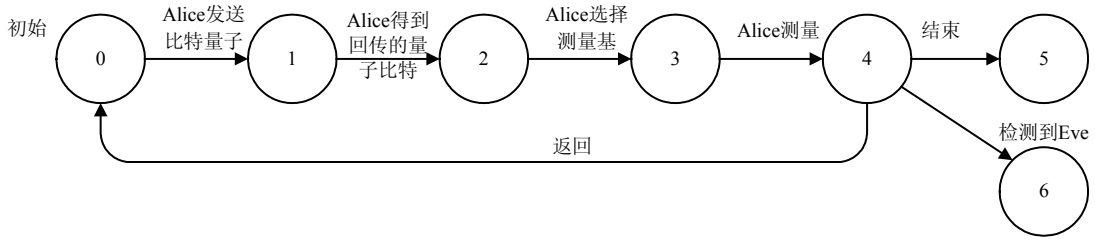

图1 Alice模块

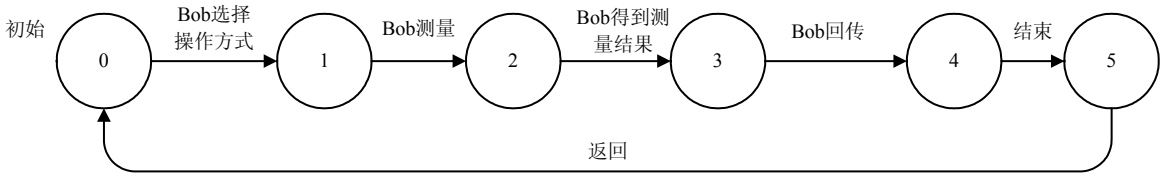

图2 Bob模块

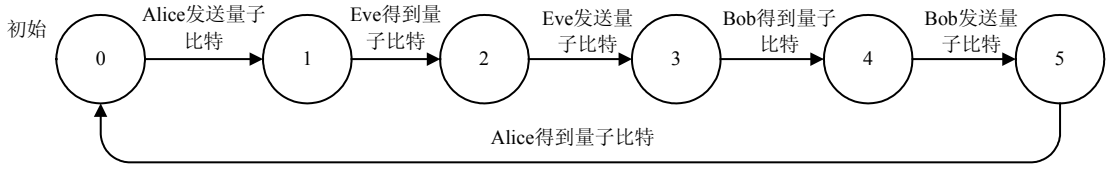

图3 信道模块

4) 窃听者模块(Eve)

由于存在多种攻击方式，不同的攻击方式中对Eve的建模过程和描述均存在不同，将在下一小节中具体讨论。

3.2 攻击描述

窃听是借助技术设备和手段，窃取语言信息、数据、文字、图像等在合法用户中传输的秘密信息。现存的攻击的方法有很多，本文对截获重传攻击、随机替换攻击和一般攻击这3种常见的攻击进行分析。

3.2.1 截获重传攻击(intercept-resend attack)

执行过程：Alice将光子传送入信道后，Eve对该光子进行截获，再随机选择一组基对该光子进行测量并记录结果。随后Eve制备一个新的与测量结果相同的光子并传入信道。

本文采用3.1节中的描述方法来描述该攻击过程。Eve的初始状态为“0”，如图4所示。

1) Eve选择测量基，状态迁移到“1”；2) Eve对光子进行测量并记录结果，状态分别由“1”变为“2”，再变为“3”；3) 当Eve制备光子并传回到信道中，整个模块回到“0”。

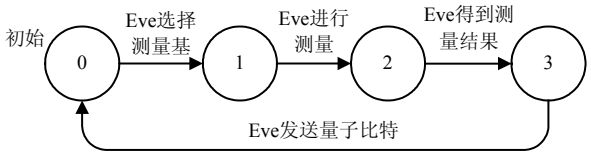

图4　截获重传攻击

3.2.2 随机替换估计(random substitute attack)

执行过程：Alice将光子传送入信道后，Eve对该光子进行截获，再随机选择一组基对该光子进行测量并记录结果。随后Eve随机制备一个新量子比特并传入信道。同样的，模块的初始状态为“0”，如图5所示。

1) Eve随机选择测量基，状态由“0”迁移到“1”；2) Eve对光子进行测量，状态由“1”变为“2”；3) Eve得到测量结果，状态迁移到“3”；4) Eve将随机制备的光子传回到信道，模块状态回到初始“0”。

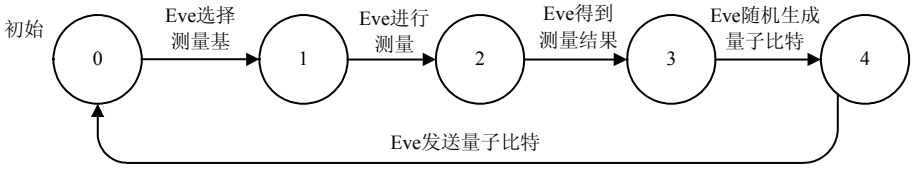

图5　随机替换攻击

3.2.3 一般攻击(general attack)

一般攻击包含前述两种攻击方式。Eve以概率PROB(1≤PROB≤1)选择截获重传攻击，或者以概率(1–PROB)选择随机替换攻击。

执行过程为：1) 当Eve选择测量基后，状态由初始状态“0”迁移到“1”；2) Eve对光子进行测量，状态变为“2”；3) Eve得到测量结果，状态变为“3”；4) Eve进行攻击方式选择，模块状态迁移到“4”；5) 当Eve把光子传回到信道后，状态回到“0”。如图6所示。

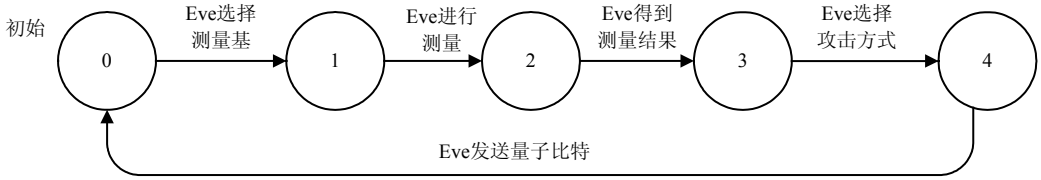

图6　一般攻击

4 验证结果

量子安全协议的目的是为了抵抗窃听者的攻击。为了将Eve检测出来，采取的方案是计算信道传输中的错误率。根据协议，在Bob没有放弃该次循环和没有噪声干扰的情况下，假如 $k_B=0$，则Bob传送的量子比特为 $|+\rangle$；假如 $k_B=1$，那么Bob发送的量子比特为 $|0\rangle$。于是可以得到，若Alice的测量结果是 $|-\rangle$，那么Bob令 $k_B=1$(若Bob将量子比特直接回传，那么Alice一定会测得 $|+\rangle$)；若Alice的测量结果得到 $|1\rangle$，则Bob采取直接回传的方式(即 $k_B=0$)。

若上述量子比特不满足的情况发生，则用随机事件 σ 来记录。设 σ 发生的次数为 L，则错误率为：

$$\eta = L/n \tag{1}$$

式中，n为中协议执行过程传输的光子的总数。那么检测到窃听者Eve的概率为：

$$P_{\mathrm{det}}(n)=P_{\mathrm{r}}\{\eta \geqslant T\} \tag{2}$$

式中，参数T是一个预先设置好的阈值。在无噪声干扰的信道中，$T=\varepsilon$。ε是一个无穷小量，其取值范围可以根据不同的安全需求进行更改。而在有噪声干扰的信道中，T取2%～8.9%[29]。图7给出了无噪声信道中上述3种攻击方式下检测到Eve的概率。

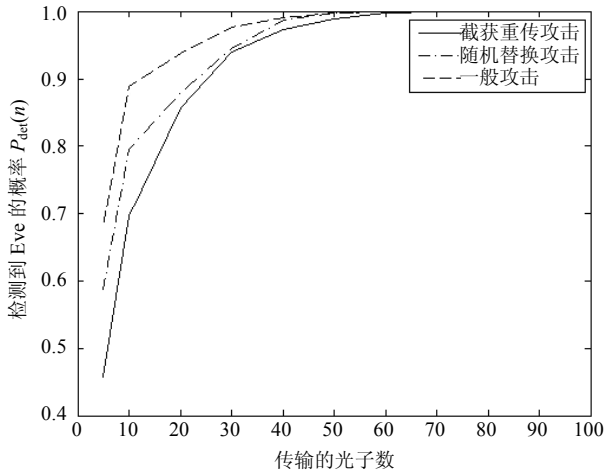

图7 验证结果I(无噪声)

从图7的结果可知，传输的光子数较少时，检测到Eve的概率较低，而当传输的光子数达到50时，检测到Eve的概率已经很接近于1；当继续增加传输的量子数时，检测概率持续上升并无限趋近于1。

在实际中，无噪声的信道是不存在的，真实信道中的噪声总是存在的。为了验证在有噪声干扰的情况下协议的安全性，需将PRISM中对信道的描述进行更改，就可以计算在噪声干扰的条件下，检测到窃听者的概率。

假设信道在由状态“0”迁移到状态“1”时噪声产生干扰(如图3所示)。在无噪声信道中，该操作可以表达为：

$$[\mathrm{aliceput}]\ \mathrm{cs}=0\rightarrow(\mathrm{cs}'=1)\&(\mathrm{cd}'=\mathrm{ad})\&(\mathrm{cb}'=\mathrm{ab}) \tag{3}$$

式中，cs表示信道的状态；cd是信道的数据；cb表示信道的测量基；ad表示Alice的数据；ab表示Alice选择的测量基。当加入噪声后，该描述变为：

$$\begin{aligned}[\mathrm{aliceput}]\mathrm{cd}=0\rightarrow\ & 0.7:(\mathrm{cs}'=1)\&(\mathrm{cd}'=\mathrm{ad})\&(\mathrm{cb}'=\mathrm{ab})+\\ & 0.1:(\mathrm{cs}'=1)\&(\mathrm{cd}'=\mathrm{ad})\&(\mathrm{cb}'=1-\mathrm{ab})+\\ & 0.1:(\mathrm{cs}'=1)\&(\mathrm{cd}'=1-\mathrm{ad})\&(\mathrm{cb}'=\mathrm{ab})+\\ & 0.1:(\mathrm{cs}'=1)\&(\mathrm{cd}'=1-\mathrm{ad})\&(\mathrm{cb}'=1-\mathrm{ab})\end{aligned} \tag{4}$$

由式(3)、式(4)可以得到，信道状态迁移到正确状态的概率为0.7，迁移到错误状态的概率为0.3。此处的错误状态有3种，分别为：选择了错误的测量基、得到错误的数据、或者两者都有。图8为有噪声时的验证结果。

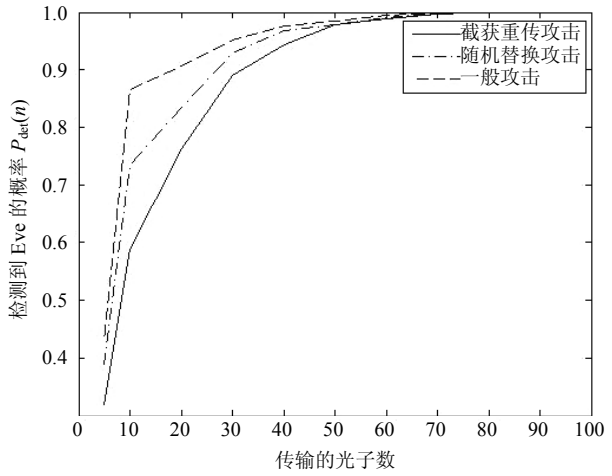

图8 验证结果II(有噪声)

从图8可以得到，在存在噪声干扰的条件下，且信道中传输的光子数较少时，检测到窃听者的概率依然较低，并且出现了下降(即比无噪声时低)。当传输的光子数增加到50个左右时，检测概率已接近于1；当传输的光子数持续增加时，检测到Eve的概率也持续上升且无限趋近于1。

5 结 束 语

本文使用了基于概率的模型检测器PRISM对半量子密钥分发协议的安全性进行验证。所采用的技术是通过抽象方法对协议执行的过程和攻击过程建立起对应的模型。现在针对量子密码协议安全性验证的方法绝大多数是采用数学证明的方法，这要求协议的设计者具备很扎实的数学功底。本文采用的模型检测方法则是一种全自动化的工具，通过抽象的方法对协议执行的过程和攻击过程建立起对应的模型，再使用相应的模型检测器就可以得到验证解结果。这就避免了使用传统方法验证的复杂程度和对个人能力的要求，提高了整个验证过程的速度和效率。验证结果表明，无论在有无噪声干扰的信道中，随着传输光子数的增多，针对截获重传攻击、随机替换攻击和一般攻击这3种攻击方式来说，检测到窃听者Eve的概率会无限趋近于1。在有噪声干扰的信道中，传输光子数较少时，Eve的检测概率会出现下降，但当传输的光子数达到足够多时，检测到窃听者的概率会逐渐增大并无限趋近于1，这证明了该半量子密钥分发协议是安全的。对于其他不同的攻击方法，依然能够使用PRISM来进行安全性的验证。同样的，量子密码协议的其他方面性质的验证

也可以使用PRISM来进行。

参 考 文 献

[1] BENNETT C H, BRASSARD G. Quantum cryptography: Public key distribution and coin tossing[C]//In Proc of IEEE International Conference on Computers, Systems, and Signal Processing. Bangalore, India: IEEE, 1984: 175-179.

[2] BENNETT C H, BESSETTE F, BRASSARD G, et al. Experimental quantum cryptography[J]. Journal of Cryptology, 1992, 5(1): 3-28.

[3] HILLERY M, BUZEK V, BERTHIAUME A. Quantum secret sharing[J]. Physical Review A, 1999, 59(3): 1829-1834.

[4] SHI R H, HUANG L S, YANG W, et al. Multiparty quantum secret sharing with Bell states and Bell measurements[J]. Optics Communications, 2010, 283(11): 2476-2480.

[5] RAHAMAN R, PARKER M G. Quantum scheme for secret sharing based on local distinguishability[J]. Physical Review A, 2015, 91(2): 91. 022330.

[6] CHUANG I, GOTTESMAN D. Quantum digital signatures: US, US 7246240 B2[P]. 2007.

[7] ZENG G H, CHRISTOPH K. An arbitrated quantum signature scheme[J]. Physev A, 2002, 65: 042312.

[8] BOYER M, KENIGSBERG D, MOR T. Quantum key distribution with classical bob[C]//First International Conference on Quantum, Nano, and Micro Technologies, 2007, ICQNM'07. [S.l.]: IEEE, 2007, 99(14): 10-10.

[9] KRAWEC W. Mediated semiquantum key distribution[J]. Physical Review A, 2015, 91(3): 032323.

[10] BOYER M, GELLES R, KENIGSBERG D, et al. Semiquantum key distribution[J]. Phys Rev A, 2009, 79: 032341.

[11] YU K F, YANG C W, LIAO C H, et al. Authenticated semi-quantum key distribution protocol using Bell states[J]. Quantum Information Processing, 2014, 13(6): 1-9.

[12] KRAWEC W. Mediated semiquantum key distribution[J]. Physical Review A, 2015, 91(3): 032323.

[13] KRAWEC W. Security proof of a semi-quantum key distribution protocol to appear[C]//IEEE ISIT 2015. [S.l.]: IEEE, 2015.

[14] KRAWEC W. Semi-quantum key distribution[D]. [S.l.]: Stevens Institute of Technology, 2015.

[15] KRAWEC W. Security of a semi-quantum protocol where reflections contribute to the secret key[J]. Quantum Information Processing, 2015, 15(5): 1-24.

[16] KRAWEC W. Restricted attacks on semi-quantum key distribution protocols[J]. Quantum Information Processing, 2014, 13(11): 2417-2436.

[17] BAIER C, KATOEN J P. Principles of model checking [M]. Cambridge, USA: The MIT Press, 2008.

[18] EMERSON E A, CLARKE E M. Characterizing correctness properties of parallel programs using fixpoints[M]//Automata, Languages and Programming. Berlin, Heidelberg: Springer-Verlag, 1980: 169-181.

[19] CLARKE E M, EMERSON E A. Design and synthesis of synchronization skeletons using branching time temporal logic[J]. Proc Workshop on Logic of Programs, 1982, 131: 52-71.

[20] CLARKE E M, EMERSON E A, SISTLA A P. Automatic verification of finite-state concurrent systems using temporal logic specifications[C]//ACM Transactions on Programming Languages and Systems. New York: ACM, 1986: 244-263.

[21] QUEILLE J P, SIFAKIS J. Specification and verification of concurrent systems in CESAR[C]//In Proc 5th Colloquium on Int Symp Programming. London: Springer, 1982: 337-351.

[22] BASAGIANNIS S, KATSAROS P, POMBORTSIS A. Synthesis of attack actions using model checking for the verification of security protocols[J]. Secur Comm Networks, 2011, 4(2): 147-161.

[23] BEN-ARI M, PNUELI A, MANNA Z. The temporal logic of branching time[J]. Acta Informatica, 1983, 20(3): 207-226.

[24] GASTIN P, ODDOUX D. Fast LTL to büchi automata translation[J]. Lecture Notes in Computerence, 2001, 2102: 53-65.

[25] YANG J, SEGER C H J. Generalized symbolic trajectory evaluation - abstraction in action[M]//Formal Methods in Computer-Aided Design, LNCS. Berlin, Heidelberg: Springer-Verlag, 2002: 70-87.

[26] YANG F, YANG G W, HAO Y J, et al. Security analysis of multi-party quantum private comparison protocol by model checking[J]. Modern Physics Letters B, 2015, 29(18): 717-755.

[27] YANG F, YANG G W, HAO Y J. The modeling library of eavesdropping methods in quantum cryptography protocols by model checking[J]. International Journal of Theoretical Physics, 2016, DOI: 10.1007/s10773-016-2969-z.

[28] ELBOUKHARI M, AZIZI M. Analysis of the security of bb84 by model checking[J]. International Journal of Network Security & Its Applications, 2010, 2(2): 87-98.

[29] CHANG Y J, TSAI C W, HWANG T. Multi-user private comparison protocol using GHz class states[J]. Quantum Information Processing, 2013, 12(2): 1077-1088.

编 辑 漆 蓉