漫谈量子保密通信的中间人攻击问题

龙桂鲁

（1. 低维量子物理国家重点实验室、清华大学物理系 100084；2. 教育部量子信息前沿中心 100084；
3. 北京信息科学与技术国家研究中心 100084；4. 北京量子信息科学研究院 100193）

量子保密通信主要包括量子密钥分发[1][2]和量子直接通信[3][4][5]。Bennett和Brassard在1984年提出的量子密钥分发，实际上是密码学中的密钥协商，Alice和Bob双方传输随机数，在确定其安全后，将传输的随机数升级为密钥，用于经典保密通信。密码学中的密钥分发是把事先确定好的密钥传送给指定的接收方。不过由于历史原因，大家一直这么称呼。由于称呼的不同，有时候会引起密码学家对量子密钥分发的误解。量子直接通信，简称量子直通，在量子信道直接安全地传输信息，是清华大学学者在2000年提出的[3]。这是信息论意义上的通信，它直接传输有意义的信息，也可以传输事先确定的密钥。量子信道指的是用于携载信号的量子态以及传输它们的介质，如用单光子极化量子态在光纤中传输，就给出了一个量子信道。经典通信本身不考虑安全性，考虑的是如何把信息可靠的传输到目的地。著名的香农理论保证了信息的可靠传输，即在信道容量大于零时，总可以找到一个编码，以小于或者等于信道容量的速率可靠的通信。量子直通是在有噪声和窃听的信道下，既可靠又安全地通信。

有一个说法是量子保密通信无法抵御中间人攻击，即窃听者在通信线路的中间假装是通信的合法用户，来套取通信双方的内容。这种说法最早从什么地方提出不得而知，但是影响最大的可能是著名法国通信专家Emmanuel Desurvire教授。他是掺铒放大器的发明者，获得包括富兰克林工程奖章、IEEE Tyndall奖等国际大奖。在他的《Classical and Quantum Information Theory》的最后一章，专门讲了这一攻击手段[6]。大致的方法是这样。假如Alice和Bob是合法通信双方，Eve是窃听者。Eve假装是Bob和Alice进行量子密钥分发，同时假装是Alice来和Bob进行量子密钥分发，这样Eve就可以获得双方所有的密钥和通信而不被发现，而且这也不违背量子力学的原理。

为了后面的叙述，我们先介绍公开密码体系。公开密码体系是一种经典加密和解密方法。例如，在RSA公开密码体系中，每个用户有三个参数，一个大数N，公钥E，私钥D，其中N和公钥E都是公开的，D是私钥，不公开。Alice有（Na，Ea，Da），Bob有（Nb，Eb，Db），窃听者Eve是其中的一个用户，有（Ne，Ee，De）。如果Bob要给Alice发一封加密信，内容是x，则Bob用Alice的（Na，Ea）加密，即x^Ea=C，C即是加密后的密文，Alice收到C后，利用私钥Da解密得到原文，C^Da=x。在现在的网络里，一般用公开密码体系，如RSA，SM2加密小量的密钥；用对称密码，如AES，SM1，SM4来加密大量的信息。

中间人攻击的实质就是认证问题。这里面有两个认证，一个是网络认证，即证明Alice就是使用公钥Ea的人；第二个是身份认证，即证明信息确实是拥有公钥Ea的人发出的。如果Alice和Bob已经完成身份认证和网络认证，Eve就无法对他们的量

子通信进行中间人攻击。中间人攻击这一问题在经典通信也是存在的。网络认证问题可以用西游记中的真假孙悟空例子来说明。在西游记的五十七回，六耳猕猴冒充孙悟空，两个长得一模一样的齐天大圣站在唐僧和师弟们面前，他们都分不出来哪个是真的。现在经典密码学中普遍采用的认证方法，是利用公开密码体系。公开密码体系RSA也可以做认证。假如Bob有一笔很大的款项要发给Alice，他要确认Alice是不是真的Alice。作为身份认证，Alice可用私钥加密一个认证信息A，y=A^Da，把y发送给Bob以证明她就是拥有公钥Ea的用户。Bob收到y后，利用公钥Ea解密y得到A，y^Ea=A。这一步确认了这个信息y是发自公钥为Ea的用户。但是这并不能证明这个有公钥Ea的用户就是Alice。如果另一个用户Eve假装是Alice，用她自己的私钥De加密A，得到A^De=y'，并将y'发送给Bob，Bob用Eve的公钥Ee解密y'，也可以得到A，这样Bob就无法判断哪个是真正的Alice。就像孙悟空、六耳猕猴长得一模一样、都有金箍棒，唐僧无法判断一样。在经典网络中，这一问题是靠一个大家都信任的超级网络管理者来解决的。网络超级管理者用自己的私钥Dsuper加密一个证书，上面写着证明Alice的公钥为Ea，大数为Na。他也给Bob做一个证书，证明Bob的公钥为Eb，大数为Nb。这样，任何人都可以使用超级管理者的公钥Esuper来解密这个证书，读出证书的内容，认可Ea的拥有者就是Alice。Eve得不到这样的证书，就无法假装成Alice了。在西游记中，这个超级网络管理者就是如来佛。网络管理者需要做的认证书的个数，就是网络中的用户数目，每个用户只需要有一个大数N和一个公钥E即可。

在量子保密通信中，尚没有量子版本的非对称密码体系。身份认证和网络认证可通过让Alice和Bob事先共享一组密钥K来解决。由于Alice和Bob事先见过，他们能够肯定掌握这组密码的人就是Alice和Bob，这样解决了网络认证的问题，即拥有这组密码的人就是Alice和Bob。Alice和Bob有这组密钥，而Eve没有，这样Bob让Alice发来共享的密钥K，就可证明发信息的人是Alice。当然Alice发送的时候，一定要保密，不然的话，Eve得到了这个共享密钥，就可以假装成Alice，使得Bob无法判断真假。在西游记中就有生动的例子，本来唐僧或者观音菩萨可以采用念紧箍咒，看是否头疼的方法来判断，只有真的孙悟空才会头疼。如果他用这个方法分别地来测试，就可以判断真假。但是他把两个猴子叫到一起，这时候六耳猕猴就偷偷地学孙悟空装疼，躲过了甄别。

采用共享密钥的方法进行认证，比用公开密钥生成证书的方法要复杂。任何两个用户都需要共享一组密钥，这样，整个网络里需要共享的密钥数量就是N(N-1)/2，也就是N的平方量级，N是网络的用户数量。对于一个拥有5万用户的网络，采用公开密码方法生成证书的方法认证，只需要发放5万个证书，而采用互相共享密钥的方法，则需要共享的25亿组密钥，大大增加了复杂度。

如果Alice和Bob事先没有共享密钥K，他们可以通过都信任的第三方Charlie来完成。Charlie可以分别和Alice和Bob进行保密通信，例如可以采用量子密钥分发+一次一密经典加密通信，或者量子直接通信，让Alice和Bob共享密钥，以便他们完成认证。这样Charlie要首先和每个用户都建立一组密钥，任何其他两个用户想进行认证，都需要Charlie来帮助他们，共享一组密钥。其数量和事先见面共享密钥的数量一样，也是平方的复杂度。

总之，量子保密通信中，由于网络认证和身份认证出现的中间人攻击是可以解决的。并不像Emmanuel Desurvire教授书中说的那样没有解决。经典认证和量子认证各有自己的优缺点。基于RSA等公开密码体系的身份认证体系在复杂度上更有优势，适合在大型网络中使用。但是由于经典密码算法的绝对安全性没有得到证明，即使现在发展的后量子密码算法，也无法证明其绝对安全性，就像NIST负责后量子密码的首席科学家Dustin Moody所说，因为担心未来有人破解，所选择的候

选后量子密码算法选择了多种途径。而采用量子通信来建立的网络认证和身份认证，其安全性在原理上已经得到了证明，其缺点是复杂度高，不利于在大型网络中使用。因而在实际应用中，可以根据其不同的使用场景，选择相应的认证方法。

参考文献

① Bennett C H, Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces. 1984.

② Ekert A K. Quantum cryptography based on Bell's theorem. Physical review letters, 1991, 67(6): 661.

③ Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. Physical Review A, 2002, 65(3): 032302.

④ Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein- Podolsky- Rosen pair block. Physical Review A, 2003, 68(4): 042317.

⑤ Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Physical Review A, 2004, 69(5): 052319.

⑥ Desurvire E. Classical and quantum information theory: an introduction for the telecom scientist. Cambridge university press, 2009.