doi: 103969/j. issn. 0490-6756. 2016. 01. 015

SIP 协议量子身份认证与密钥协商方案

杨　光[1,2]，聂　敏[1]，杨武军[1]
(1. 西安邮电大学通信与信息工程学院，西安 710121；2. 西北工业大学电子信息学院通信工程系，西安 710072)

摘　要：针对现有 SIP 协议安全方案无法检测窃听、以及经典密码体制面临量子计算攻击时的脆弱性问题，提出了一种将量子用户身份认证及密钥协商与 SIP 协议结合的方案。SIP 服务器制备三粒子 W 态并将其中两个粒子分发给 SIP 用户，首先对随机插入的粒子进行测量以检测窃听，然后通过量子操作与测量验证用户身份；密钥协商阶段，三方不需制备与分发新的 W 态，仍基于持有的 W 态进行随机测量，SIP 用户根据有效测量结果生成初始会话密钥. 性能分析表明本方案能够对抗伪装攻击与窃听攻击，有效提高 SIP 协议安全性。

关键词：量子通信；会话启动协议；身份认证；密钥协商
中图分类号：TN918. 91　　**文献标识码**：A　　**文章编号**：0490-6756(2016)01-0087-06

Quantum authentication and key agreement scheme for SIP protocol

YANG Guang[1,2], *NIE Min*[1], *YANG Wu-Jun*[1]
(1. School of Communication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China; 2. Department of Communication Engineering, School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract: To overcome the shortcomings of current SIP safety scheme, such as the incapability to detect the wiretap and the vulnerability of the classical key system in case of quantum computation attack, this paper proposes a novel user authentication and key agreement scheme that combined quantum safe communication methods and SIP protocol. The SIP server prepared the three particle W states and distributed two of them to the SIP users. The random inserted particles were measured first to detect the wiretap; then the rest of the W states were operated and measured to authenticate the user. After that, every particle of the W states was measured randomly and the two SIP users got the initial conversation key according to the results of the effective measurements. The performance analysis shows our scheme is capable of resisting the impersonation attack and wiretap attack, thus can increase the safety of SIP protocol effectually.

Key words: Quantum communication; SIP; Authentication; Key agreement

1　引言

会话启动协议(Session Initiation Protocol, SIP)是 IETF 提出的一种在因特网上实现多媒体会话的应用层信令控制协议. 因其简单、易于扩展等优势，已成为下一代网络及移动 IP 多媒体子系统中的一个重要协议[1]. 由于 SIP 协议消息是通过 IP 网承载的，且消息编码采用简单的文本形式，其

收稿日期：2014-12-22
基金项目：国家自然科学基金(61172071,61201194)；陕西省自然科学基础研究计划(2014JQ8318)；陕西省国际合作与交流计划项目(2015KW-013)；陕西省工业攻关项目(2014K09-14)
作者简介：杨光(1977－)，女，博士研究生，讲师，主要研究领域为网络协议、量子通信. E-mail: Guangyanging@163. com

消息传递需经过注册服务器、重定向服务器等多个中介和不信任域,协议实体通信过程可能遭遇多种安全问题,如欺骗、窃听、会话篡改等.因而,如何保证SIP网络的安全性成为近年来的研究热点.现有的SIP安全解决方案有HTTP摘要式认证[2]、基于PKI公钥体制的认证机制[3]、基于双线性对技术的身份认证与密钥协商[4]机制、基于口令的身份认证与密钥协商机制等[5].

然而,现有的SIP安全机制存在的主要问题是:无法检测窃听,而且经典密码体制意义上的安全性是以破解密码的计算复杂度为前提的.1994年Shor量子算法[6]的发现,对基于数学算法的经典加密过程产生了很大的威胁.目前已被证明,经典的RSA、DSA、ECDSA[7-8]等算法都能被量子算法轻易攻破.在不久的未来,当SIP网络面临量子计算能力的威胁与攻击,其中至关重要的身份认证信息、密钥信息可能被轻易破解.

量子通信基于海森堡不确定性原理和量子态不可克隆定理,能够实现对窃听的可检测性和无条件安全性,近年来量子安全保密通信领域引起了全球各国的高度重视.2003年,美国DARPA量子密钥分配网络开始全面运作[9];2008年,欧洲SECOQC量子通信网络开始成功运行[10];2012年我国安徽合肥46节点量子城域网开始试运行,2014年,我国国家级重大工程"量子保密通信京沪干线"项目启动,将形成大规模量子广域保密通信网,并支持金融、电子政务、多媒体等多种应用[11].量子安全保密通信技术与互联网技术的结合将成为未来量子通信网的一个发展趋势[12-14],因而将量子安全机制应用于SIP协议成为可能.但在电信级SIP网络当中,用户注册及呼叫建立、释放过程等都需要由SIP服务器进行控制,因而其中有关的认证、密钥协商等涉及到SIP用户、SIP服务器多方的参与.目前已经提出的量子密钥分发(Quantum Key Distribution,QKD)协议如BB84、B92等仅适于两方参与的安全通信,而一些三方量子QKD方案也并不能充分满足SIP协议安全机制的需求[15-16].基于此背景,本文提出了一种在SIP网络中,利用三粒子纠缠W态,在SIP服务器控制下进行的SIP用户身份认证与会话密钥协商的方案,能够克服经典SIP安全机制的不足之处,实现一次一密的SIP多媒体会话,更加有效地保障SIP协议的安全性,满足高等级IP多媒体保密通信的需求.

2 基于三粒子W态的量子认证与密钥协商方案

2.1 基于三粒子W态的量子身份认证

量子纠缠是一种重要的量子力学特性,其基本性质已经成为多种量子通信方案的基础之一.纠缠态的非经典特性表现为两个或多个纠缠的粒子不是独立的,而须被看作一个组合系统.相互关联的纠缠态中的粒子不能被简单分解为多个单粒子态的直积.不管纠缠态中的各个粒子在空间上相距多远,观测其中的一个粒子,都会改变对其余粒子测量的结果.

W态是一种多粒子非最大纠缠态,2000年由Dur[17]提出,其关键特性在于纠缠的强健性.以三粒子W态为例,在丢失任一粒子的情况下,也不会破坏剩余两粒子的纠缠特性.三粒子W态可表示为:

$$|W\rangle_{123}=\frac{1}{\sqrt{3}}(|001\rangle_{123}+|010\rangle_{123}+|100\rangle_{123}) \quad (1)$$

这里,$|0\rangle$、$|1\rangle$是二维量子状态空间的基矢,实际的物理系统可以是电子两自旋态、光子两偏振态或原子两能级态.下标1、2、3分别代表W态中三个纠缠粒子的编号.

在一次量子认证过程中,有三个参与方:通信用户Alice、Bob及认证管理者Charlie.假定Charlie是可信的,需要被认证的是Alice与Bob.

在进行认证之前,需要事先在Alice与Charlie、Bob与Charlie之间共享各自的身份秘密比特串I_A及I_B,并假定I_A及I_B等长且长度为L.以对Alice的身份认证为例,认证过程包括以下步骤:

(1)由Charlie制备L个三粒子W态,$|W\rangle_{1i,2i,3i}$,$i=1,2\ldots,L$,并根据I_A及I_B、对$|W\rangle_{1i,2i,3i}$中的粒子1_i和粒子2_i依次进行I操作或X操作.以I_A为例,假如I_A第i比特为0,则进行I操作;为1则进行X操作.其中,I操作与X操作定义为

$$I=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \quad (2)$$

在进行操作后,原有的$|W\rangle_{1i,2i,3i}$态变为:

$$|W\rangle_{1i,2i,3i}'=[(1-I_{Ai})I+I_{Ai}X]\otimes[(1-I_{Bi})I+I_{Bi}X]|W\rangle_{1i,2i,3i} \quad (3)$$

(2)为检测信道上的窃听,Charlie继续制备R个三粒子W态,并随机将其插入到操作后的L个三粒子序列中,并记录插入位置.接下来,Charlie

依次将 $L+R$ 个三粒子序列中的粒子 1_i 分发给 Alice，粒子 2_i 分发给 Bob，粒子 3_i 保留在自己手中.

(3) Charlie 在公开信道上公布 R 个 W 态的插入位置，并要求 Alice 及 Bob 随机地沿 X 或 Z 方向测量这些位置上对应的粒子 1_i、2_i，并公布测量结果与测量基.

这里，沿 X 方向测量表示使用 $|+\rangle$、$|-\rangle$ 基进行测量；沿 Z 方向测量表示使用 $|0\rangle$、$|1\rangle$ 基进行测量. 此处 $|+\rangle$、$|-\rangle$ 基为二维量子状态空间的另一组完备正交基，且满足如下关系：

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) \tag{4}$$

(4) Charlie 根据 Alice、Bob 公布的测量基选择适当的测量基，测量自己插入位置上的 R 个粒子 3_i，并判断 Alice、Bob 及自己的测量结果是否违背 CH-Bell[18] 不等式，如果不违背则说明三粒子态并不是 W 态. 当非 W 态的个数超过一定的门限，则认为信道上存在窃听，结束本次认证过程. 否则，执行 5)

(5) 对于剩余的 L 个三粒子态，Alice 根据 I_A 依次对收到的粒子 1_i 进行 I 操作或 X 操作，Bob 根据 I_B 依次对粒子 2_i 进行 I 操作或 X 操作.

操作后，粒子 1_i、2_i、3_i 所处的状态变为

$$\begin{aligned}|W\rangle_{1i,2i,3i}'' = {} & [(1-I_{Ai})I + I_{Ai}X] \otimes [(1-I_{Bi})I + I_{Bi}X] \\ & \otimes [(1-I_{Ai})I + I_{Ai}X] \otimes \\ & [(1-I_{Bi})I + I_{Bi}X]\,|W\rangle_{1i,2i,3i} = |W\rangle_{1i,2i,3i}\end{aligned} \tag{5}$$

即，如果 Alice 及 Bob 为合法用户，则粒子 1_i、2_i、3_i 所处的状态还原为 W 态.

(6) 接下来 Alice、Bob、Charlie 分别对自己持有的粒子进行测量.

(7) Bob 要求 Charlie 与 Alice 先后公布对拥有的粒子 3_i、1_i 的测量结果，并根据自己对粒子 2_i 的测量结果判断这些三粒子态是否处于 W 态. 如果非 W 态的个数超过一定的门限值，可判断 Alice 为非法用户，则通信过程终止. 否则 Alice 为合法用户，继续执行后续量子密钥协商过程，并在公开信道上发出通知，要求三方丢弃非 W 态的粒子.

2.2　基于三粒子 W 态的量子密钥协商

假定经过 2.1 所述的身份认证过程，Alice 及 Bob 为合法用户，则 Alice、Bob、Charlie 所持的粒子 1_i、2_i、3_i 仍处于 W 态. 接下来，并不需要重新制备新的 W 态，而是继续利用当前持有的 W 态，在 Charlie 控制下，完成 Alice、Bob 间后续通信的会话密钥协商.

三粒子 W 态可重新表述为[19]：

$$\begin{aligned}|W\rangle_{123}'' &= \frac{1}{2\sqrt{3}}[(2|+\rangle_1|+\rangle_2 - 2|-\rangle_1|-\rangle_2)|0\rangle_3 \\ &\quad + (|+\rangle_1 + |-\rangle_1)(|+\rangle_2 + |-\rangle_2)|1\rangle_3] \\ &= \frac{1}{2\sqrt{3}}[(2|+\rangle_1|+\rangle_3 - 2|-\rangle_1|-\rangle_3)|0\rangle_2 \\ &\quad + (|+\rangle_1 + |-\rangle_1)(|+\rangle_3 + |-\rangle_3)|1\rangle_2] \\ &= \frac{1}{2\sqrt{3}}[(2|+\rangle_2|+\rangle_3 - 2|-\rangle_2|-\rangle_3)|0\rangle_1 \\ &\quad + (|+\rangle_2 + |-\rangle_2)(|+\rangle_3 + |-\rangle_3)|1\rangle_1]\end{aligned} \tag{6}$$

根据式(6)，当 Alice、Bob、Charlie 对自己持有的粒子进行随机测量，可以选择的测量方向为 X 或 Z 方向，则 Alice、Bob、Charlie 可能选择的测量方向组合有 8 种，分别是 (Z,Z,Z)、(Z,Z,X)、(Z,X,Z)、(Z,X,X)、(X,Z,Z)、(X,Z,X)、(X,X,Z)、(X,X,X). 但其中可用测量基组合只有三种，分别为 (X,X,Z)、(X,Z,X) 及 (Z,X,X). 以测量方向 (X,X,Z) 为例，当 Charlie 沿 Z 方向测量自己所持的粒子 3_i 的结果为 $|0\rangle$，则粒子 1_i、2_i 处在纠缠态 $|+\rangle_1|+\rangle_2 - |-\rangle_1|-\rangle_2$ 上，即粒子 1_i、2_i 总是处在相同的量子态；若 Charlie 沿 Z 方向测量的结果为 $|1\rangle$，则粒子 1_i、2_i 所处的状态不确定.

根据以上原理，基于 W 态的密钥协商过程如下.

(1) 对于每一个 $|W\rangle_{1i,2i,3i}$ 态，Alice、Bob、Charlie 随机沿 X 方向或 Z 方向测量自己所持的粒子，并通过公开信道公布自己的测量基；

(2) Alice、Bob、Charlie 判断三方公布的测量基组合状态，若为 (X,X,Z) 的测量，则保留其测量结果，并执行步骤 3)，否则返回步骤 1)；

(3) Charlie 公布自己沿 Z 方向的测量结果. 若结果为 $|0\rangle$，则 Alice 及 Bob 保留他们对应的测量结果并作为初始会话密钥，并执行步骤 4)；若 Charlie 测量结果为 $|1\rangle$，则 Alice 及 Bob 放弃其测量结果并返回步骤 1)；

(4) Alice、Bob、Charlie 判断是否已经测量完自己持有的所有的粒子，如果测量完，则执行步骤 5)，否则返回步骤 1)；

(5) Alice 及 Bob 根据事先约定的密钥扩展算法，对协商产生的初始会话密钥进行扩展，得到后续媒体会话所需的完整会话密钥.

3 基于量子认证与会话密钥协商的 SIP 协议工作过程

图 1 给出了基于量子身份认证与密钥协商的 SIP 呼叫基本流程. 在认证与密钥协商过程中,假设 SIP 注册服务器与 SIP 代理服务器是位于同一服务器上的,以下简称 SIP 服务器. 在基于量子认证与密钥协商的 SIP 网络中,每个新入网的用户需从 SIP 网络服务器获取自己的身份证书 P 及单值散列函数 H,利用散列函数 H 计算身份摘要信息 $I=H(P)$. 在身份认证过程中,用户只需要采用量子认证方式传递身份证书摘要信息 I,从而使得证书信息不直接用于编码,进一步增强身份信息的传输安全性与传输效率. 完整的量子 SIP 网络身份认证与会话密钥协商由经典 SIP 协议流程与量子通信过程结合而成. 其中涉及量子信道与经典信道两种通信信道. W 态粒子的分发采用量子信道,其余信息的传送采用经典信道. 一个具体的呼叫过程如图 1 所示.

在图 1 中,Alice 为主叫用户,Bob 为被叫用户,Charlie 为 SIP 服务器. SIP 呼叫方式采用代理呼叫过程,SIP 服务器需进行信令转发.

首先,Alice 通过经典方式发送 Invite 消息,服务器 Charlie 解析并转发该消息给 Bob. 如果 Bob 需要认证 Alice 身份,则返回 401 未授权消息,要求 Alice 提供身份认证信息. Alice 同意进行认证且返回 ACK 消息。

接下来,由 SIP 服务器制备 L 个三粒子 W 态,并另外制备 R 个三粒子 W 态用于检测窃听。在 SIP 服务器控制下,三方进行窃听检测,并根据身份证书摘要信息 I_A 及 I_B 执行对用户 Alice 的量子身份认证过程. 如果 Alice 身份认证成功,则 Alice、Bob、Charlie 持有的粒子仍处在 W 态。

利用这些 W 态,Alice 与 Bob 继续进行密钥协商,生成一致的初始会话密钥,并经过密钥扩展获得完整会话密钥,用于对后续通信的经典媒体消息进行加密,实现一次一密的 SIP 媒体会话。

4 方案性能分析

4.1 量子身份认证安全性

4.1.1 窃听检测性能分析 在经典 SIP 认证过程中,窃听是无法检测的. 但在本文量子认证方案中,窃听是能够检测的.

这里以最常见的截获—重发攻击为例. 如果

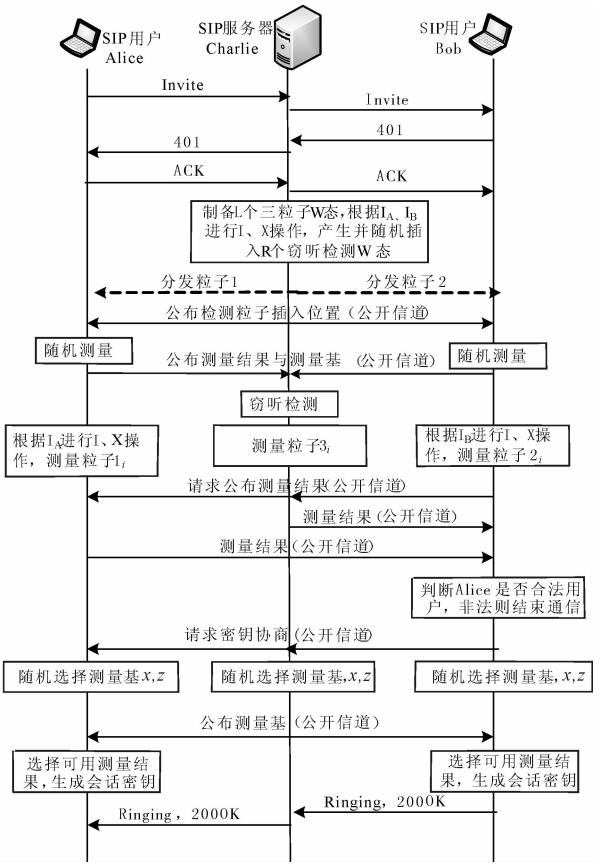

图 1 基于量子身份认证与密钥协商的 SIP 呼叫过程(图中实线代表经典信道,虚线代表量子信道)

Fig. 1 SIP calling process based on quantum authentication and key agreement (The solid lines signify the classical channel, the dotted lines signify the quantum channel)

存在 Eve 进行认证信息窃听,则 Eve 对量子信道的窃听发生在 Charlie 向 Alice、Bob 分发粒子的阶段. 由于 Eve 事先并不知道哪些粒子是用于检测窃听的,哪些是用于身份认证的,所以 Eve 只能对所有截获到的粒子 1_i、2_i 进行测量,并根据测量结果产生两个新的粒子 1_i^* 2_i^* 然后分发给 Alice 及 Bob. 假设 Eve 对截获的粒子 1_i、2_i 的测量结果为 $|00\rangle$,且该粒子对为 R 个检测粒子对中的一对,则此时 Charlie 持有的粒子 3_i 位于态 $|1\rangle$. 接下来,Eve 产生两个粒子,其量子态分别为 $|0\rangle$、$|0\rangle$,并重新分发给 Alice 及 Bob,但这两个粒子与 Charlie 持有的粒子 3_i 已经不再具有纠缠关系,即三粒子所处的态已成为经典态. 当 Charlie 要求 Alice、Bob 公布对所持粒子的测量结果及测量基,并与自己的测量结果进行判断时,将不再违背 CH-Bell 不等式,因而 Charlie 会检测到非法态的存在. 考虑到量子信道上的差错,当非法态的个数超过事先规定

的门限值，就可以明确地判断出窃听者 Eve 的存在.

门限值的选择对窃听检测结果具有重要的影响. 当门限值过高，将增加检测的漏检率；门限值过低则会增加检测的虚警率. 这里影响门限值的主要因素是量子信道的差错率. 设可用量子信道的量子比特差错率为 λ_{QBER}，则采用 R 个三粒子 W 态进行窃听检测检时，非法态门限值 N_{eth} 应满足式(7).

$$\frac{N_{\mathrm{eth}}}{R} \leqslant 2\lambda_{\mathrm{QBER}} - \lambda_{\mathrm{QBER}}^2 \tag{7}$$

4.1.2　*抗伪装攻击性能分析*　假设非法用户 *David* 伪装成 *Alice* 接入 *SIP* 系统，并试图呼叫 *Bob*. 则根据本文认证过程，*David* 可以获得由 *Charlie* 分发的三粒子 W 态中的粒子 1_i，但由于 David 不具有 Alice 的证书且不知道单值散列函数 $H(P)$，因此无法获取证书摘要信息 I_A. 因此 David 只能随机地对粒子 1_i 进行 I 操作或 X 操作. 假定原来 Charlie 根据 I_A 对粒子 1_i 进行了 X 操作，而 David 选择对粒子 1_i 进行 I 操作，则在最后测量前，无法将粒子 1_i 的状态恢复为原有状态，而是相当于对粒子 1_i 进行了 X 操作，这样粒子 1_i、2_i、3_i所处的状态变为：

$$[\varphi]_{1i,2i,3i} = \frac{1}{\sqrt{3}}[101]_{1i,2i,3i} + [110]_{1i,2i,3i} + [000]_{1i,2i,3i} \tag{8}$$

根据式(8)，当 David、Charlie 公布对粒子 1_i、3_i 的测量结果，Bob 根据自己的测量结果可以发现出现了非法态 $[101]$、$[110]$、$[000]$. 当非法态的个数超过事先规定的门限值，则认证失败，David 为非法用户.

由于 David 对粒子 1_i 随机地选择 I 操作或 X 操作，对于每一个粒子，设其选对操作的概率为 p_s. 假设 David 每次操作选择是独立同分布的，且摘要信息 I_A 的长度为 L. 则 David 在一次身份认证过程中，出现非法态的平均个数为：

$$N_{\mathrm{error}} = \sum_{i=0}^{L} iC_L^i(1-p_s)^i p_s^{L-i} = Lp_s \tag{9}$$

根据式(9)，可以设定非法态门限值 N_{th} 应满足

$$\frac{N_{\mathrm{error}}}{K} - 1 \leqslant N_{th} \leqslant \frac{N_{\mathrm{error}}}{K} \tag{10}$$

这里 K 为门限系数，其取值与量子信道上的差错率相关.

4.2　量子密钥协商性能分析

4.2.1　*量子密钥协商安全性分析*　在经典 SIP 用户密钥协商过程中，面临的主要安全威胁是密钥窃听. 然而根据 2.2 节的原理，由于本文密钥协商阶段所使用的三粒子 W 态是在认证阶段执行之后恢复的 W 态，而不需要重新制备 W 态并进行粒子分发，因此窃听者 Eve 无法利用粒子分发过程进行截获－重发攻击，仅可能得到公共信道上 Alice、Bob 公布的测量结果与测量基. 而由于 Alice、Bob 选择的测量基是随机的，根据这些结果无法得出 Alice 与 Bob 共享的密钥. 同时本文方案在密钥协商阶段与身份认证阶段共用 L 个三粒子 W 态，能够有效地节约量子纠缠资源.

4.2.2　*密钥生成效率*　由于在密钥协商过程中，Alice、Bob、Charlie 随机地选择测量基，因此并非每次测量都是有效的. 假定三者选择 X、Z 方向测量的概率是随机的，并且三者的测量选择过程是彼此独立同分布的，设密钥协商阶段持有的 W 态总数为 L_R 个，则根据本文密钥协商过程，Alice、Bob 协商生成的初始密钥平均长度 L_{ek} 为

$$L_{ek} = \frac{4}{5}\sum_{m=0}^{L_R} mC_{L_R}^m p_c^m (1-p_c)^{L_R-m} \tag{11}$$

上式中，p_c 为 Alice、Bob、Charlie 选择测量组合 (X,X,Z) 的概率，设三者独立选择测量基 X 的概率为 p，则：

$$p_c = p^2(1-p) \tag{12}$$

将式(12)代入(11)，得到：

$$L_{ek} = \frac{4L_R p^2(1-p)}{5} \tag{13}$$

图 2 给出了初始密钥平均长度随概率 p 变化的情况. 从图中可以看出，初始密钥平均长度大约在 $p=0.68$ 时取得最大值，密钥生成效率最高. 但当 $p=0.5$ 时，Alice、Bob、Charlie 选择测量基的随机性最强，因而密钥协商的安全性最强. 为获得最佳的密钥分配性能，可以在(0.5,0.68)的区间选择适当的 p 值.

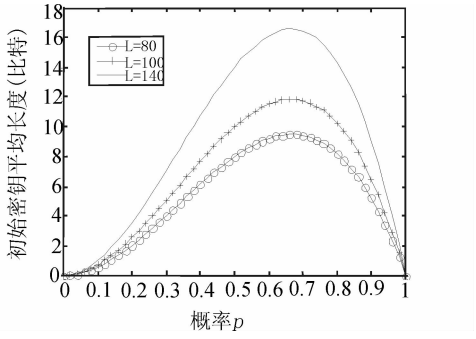

图 2　初始密钥平均长度随概率 p 的变化情况

Fig. 2　The length of initial key varying with p

5 结束语

SIP 协议在当前多媒体通信网及下一代网络中都具有重要的作用,然而传统的 SIP 安全机制无法检测窃听者的存在.一旦窃听者获取了与 SIP 用户身份及密钥相关的机密信息,就有可能通过量子算法进行破译,协议安全性将面临严重威胁.而量子保密通信具有窃听可检测性和无条件安全性,将量子安全机制与经典通信结合会有效提高通信安全性.根据 SIP 协议的工作特点,本文提出了一种基于三粒子 W 态、由 SIP 服务器控制进行的量子用户身份认证与密钥协商方案,能够有效检测窃听、对抗伪装攻击,利用量子信息的物理特性保障通信的安全性,实现一次一密的媒体会话.随着未来量子互联网的出现,如何将量子安全机制与经典网络协议进行有效结合、在增强协议安全性的同时提高方案的可操作性及效率将是下一步研究的主要内容.

参考文献:

[1] Calme J, Ejzak R. A common SIP profile for next-generation networks[J]. Bell Labs Techl J, 2006, 11(1): 107.

[2] 顾晓辉, 施佳佳, 郭放. SIP 的安全机制及其 HTTP 摘要认证的改进[J]. 东华大学学报:自然科学版, 2010, 36(2): 165.

[3] 施苑英. 一种高效的 P2PSIP 认证与密钥协商机制[J]. 计算机应用研究, 2011,28(1): 234

[4] Wang F J, Zhang Y Q. A new provably secure authentication and key agreement mechanism for SIP using certificateless public-key cryptography [J]. Comput Commun, 2008, 30(10): 2142.

[5] Yeh H T , Sun H M. Password authenticated key exchange protocols among diverse network domains [J]. Comput Electr Eng, 2005, 31: 175.

[6] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings of 35th Annual Symposium on Fundamentals of Computer Science. Santa Fe : IEEE, 1994: 124.

[7] 陈港, 胡晓勤. 一种基于 RSA 的软件保护方法[J]. 四川大学学报: 自然科学版, 2011, 48(4): 789.

[8] 乔帅庭, 韩文报, 李益发, 等. 一种改进的中间域多变量公钥签名方案[J]. 四川大学学报:自然科学版, 2014, 51(3): 512.

[9] Elliott C. The DARPA quantum network [M]. Florida: Taylor & Francis Group CRC Press,2006.

[10] Poppe A, Peev M, Maurhart O. Outline of the SECOQC quantum key distribution network in Vienna[J]. Int J Quantum Inf, 2008, 6(2): 209.

[11] 许华醒.量子通信网络发展概述[J]. 中国电子科学研究院学报, 2014, 9(3): 259.

[12] Chen T Y, Liang H, Liu Y, *et al*. Field test of a practical secure communication network with decoy state quantum cryptography [J]. Opt Express, 2009, 17(8): 6540.

[13] Chen T Y, Wang J, Liang H, *et al*. Metropolitan all-pass and inter-city quantum communication network[J]. Opt Express, 2010, 18(26): 27217.

[14] Oesterling L, Hayford D, Friend G. Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information[C] //Proceedings of 2012 IEEE Conference on Technologies for Homeland Security. Waltham: IEEE, 2012.

[15] 杨光, 聂敏, 江帆. 低轨道量子卫星通信时分交换方案及性能分析[J]. 电信科学, 2014, 30(4): 68.

[16] Elboukhari M, Azizi A, Azizi M. Quantum key distribution in practice: The state of art [C] //Proceedings of 2010 5th International Symposium on I/V Communications and Mobile Network. Rabat: IEEE, 2010.

[17] Dur W, Vidal G, Cirac J I. Three qubits can be entangled in two inequivalent ways[J]. Phy Rev A, 2000, 62(6): 062314.

[18] Cabello A. Bell's theorem with and without inequalities for the three-qubit Greenberger-Horne-Zeilinger and W states [J]. Phy Rev A, 2002, 65: 032108.

[19] 温巧燕, 郭奋卓, 朱甫臣. 量子保密通信协议的设计与分析[M]. 北京: 科学出版社, 2009.