Journal of Computer Applications
计算机应用,2015,35(4):981 -984,995
ISSN 1001-9081
CODEN JYIIDU
2015-04-10
http://www.joca.cn

文章编号:1001-9081(2015)04-0981-04
doi:10.11772/j.issn.1001-9081.2015.04.0981

基于 W 态的高效量子信息拆分方案

谢淑珍,谭晓青*
(暨南大学 信息科学技术学院,广州 510632)
(*通信作者电子邮箱 ttanxq@jnu.edu.cn)

摘　要:为提高基于 W 态的量子通信方案的效率,提出了一种新的基于 W 态的量子信息拆分(QIS)方案。该方案中,秘密分发者通过局域操作将经典信息编码在量子比特上,并在分发的量子比特中随机插入非正交态粒子进行检测窃听,参与者只需进行 3 粒子投影测量即可恢复秘密。方案使参与者能够利用 1 个 W 态直接共享 2 比特经典信息,并能够抵御截获-测量、截获-重发和纠缠附加粒子攻击,安全性得以保证。该方案效率较高,理论上其量子比特效率为 67%。

关键词:量子信息拆分;W 态;局域操作;非正交态粒子
中图分类号:TP309.7　　**文献标志码**:A

Efficient quantum information splitting scheme based on W states

XIE Shuzhen, TAN Xiaoqing*
(*College of Information Science and Technology, Jinan University, Guangzhou Guangdong 510632, China*)

Abstract: To improve the efficiency of quantum communication based on W states, a new scheme about Quantum Information Splitting (QIS) based on W states was proposed. Local operation was used to encode the classic information into the qubit by dealer in this scheme. The nonorthogonal state particles were inserted to detect eavesdropping in the distribution of qubit. To recover the secret, participants only needed to perform three-particle projective measurements. One W state can transmit two bits of classical information between the participants. Moreover, the scheme can resist some attacks like intercept-and-measure attack, intercept-and-resend attack and entangled ancillary particles attack to make sure of its security. The scheme has good efficiency with theoretical quantum efficiency of 67%.

Key words: Qantum Information Splitting (QIS); W state; local operation; nonorthogonal state particle

0　引言

随着量子密码学的不断发展,量子密码学在理论和实验上都取得了巨大的成果[1-4],其中一个研究最广的分支就是量子信息拆分(Quantum Information Splitting, QIS),也称为量子秘密共享(Quantum Secret Sharing, QSS)。它的基本思想是:Alice 想找人代她在一个远方城市做一件重要的事情(完成这件事情需要 Alice 的秘密任务信息),而她在这个城市有两个代理人 Bob 和 Charlie,但 Alice 对他们并不是完全信任。于是,Alice 可以把她的秘密信息以适当的方式进行拆分,并将拆分后的子秘密分别发给 Bob 和 Charlie,同时 Alice 确信以下两点:1)至少有一个代理人是诚实的;2)两个代理人合作可以解密出她的秘密信息,但每一个代理人都不能单独获得关于此秘密的任何信息。这样就可以保证 Alice 的任务能够顺利完成。

自从 1999 年 Hillery 等[5]利用 GHZ 纠缠态提出第一个 QIS 协议以来,越来越多的学者开始研究这个方向,并利用不同的物理性质提出了多种各具特色的 QIS 方案。2003 年 Bagherinezhad 等[6]提出基于可重用 GHZ 态的量子信息拆分方案,该方案的优点是 GHZ 态可重复使用;然而 Xie 等[7]指出若窃听者 Eve 采取纠缠附加粒子攻击(entangled ancillary particles attack),那么,他将获取奇数位的信息并不被合法通信者发现。2005 年,Deng 等[8]利用 Bell 态提出了一种高效的量子信息拆分方案,该方案通过打乱和重构 Bell 态粒子之间的对应关系实现秘密共享。随着 Dür 等[9]于 2000 年第一次提出 W 态以来,有关 W 态的各类协议也相继出现,2006 年 Agrawal 等[10]在 W 态族中找到一类可以实现隐形传态和稠密编码协议的 W 态;2007 年,Li 等[11]研究了 Agrawal 提出的 W 态,并讨论了这类 W 态和 GHZ 态之间的关系,得出这类 W 态可由 GHZ 态 $|\varphi\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$ 通过酉操作得到。2011 年 Hwang 等[12]提出了基于 GHZ 态的多方量子信息拆分方案,该方案一个 GHZ 态可共享 2 比特经典信息,但 Liu 等[13]指出参与者 Charlie 不需要做任何攻击就可获得 1 比特秘密信息,并通过增加一个局域操作来改进方案;然而 Tan 等[14]指出,Liu 的改进方案仍然是不安全的,如果 Charlie 采取截获-重发攻击(intercept-and-resend attack)[15-16],他将获得所有的秘密,并且不被检测到。

GHZ 态和 W 态是两种主要的 3 粒子纠缠态,从纠缠程度上看,GHZ 态是 3 量子比特的最大纠缠态,如果其中某个比特被探测出来,剩余两个比特也将完全失去纠缠,而 W 态虽

收稿日期:2014-10-28;**修回日期**:2014-12-19。
基金项目:国家自然科学基金资助项目(61003258, 61472165);广东省科技计划项目(2013B010401018)。
作者简介:谢淑珍(1990 -),女,江西赣州人,硕士研究生,主要研究方向:密码编码学;　谭晓青(1976 -),女,湖南衡阳人,副教授,博士,主要研究方向:密码编码学。

然不处于最大纠缠态,但比 GHZ 态更强健,在丢失一个粒子的情况下,不会影响剩余两个粒子的纠缠状态,具有较好的稳健性,而且 W 态更易于实验实现[17-20]。Zhang 等[17]采用线性光学系统产生 3 粒子 W 态,制备成功的概率高于之前的线性光学系统方案。Cardoso 等[18]提出利用腔量子电动力学(cavity Quantum ElectroDynamics, cavity-QED)制备 W 态,该方案只需一个 3 能级原子和 2~3 个腔,在当前技术条件下是可实现的。Zha 等[19]提出使用 6 粒子最大纠缠态作为量子信道可实现远程制备 W 态。林青[20]则基于交叉相位调制技术,利用两个已知的基本操作——控制路径门和融合门,实现了任意多光子 W 态的确定性制备。

从来源方面考虑,QIS 是为解决多方密钥分发问题而产生的,实际上是一种多方的密钥分发,而不是像经典秘密共享中那样直接把秘密分成多份。受量子密钥分发(Quantum Key Distribution,QKD)与经典一次一密乱码本结合的通信方式的启发,一种新的通信模式——量子安全直接通信(Quantum Secure Direct Communication,QSDC)引起了研究者的关注。QSDC 不同于 QKD 或 QIS,无需事先生成会话密钥来加密通信消息,而是直接采用量子信道进行消息的传送。由于 W 态良好的纠缠特性、制备的可行性和 QSDC 瞬时通信的特性,各类基于 W 态的 QSDC 协议也相继出现。2006 年,Cao 等[21]提出了一个基于 4 粒子对称 W 态的 QSDC 协议,实现一个 4 粒子 W 态传送 1 个经典比特信息。随即又提出一种 3 粒子对称 W 态的 QSDC 协议[22],协议中 1 个 W 态以 2/3 概率传送 1 比特信息。2008 年,Dong 等[23]提出了一个基于隐形传态的 QSDC 协议,不同于文献[22]之处在于,他们采用的是一类非对称 W 态,该协议可以实现全概率消息传送,而非以一定概率传送,不过该协议需要辅助粒子才能实现 1 个 W 态传送 1 比特信息。接着 Dong 等[24]则对文献[23]进行改进,不需要辅助粒子实现了 1 个 W 态传送 1 比特信息。2014 年,刘超等[25]提出了一种基于 3 粒子对称 W 态的 QSDC 协议,实现 1 个 3 粒子 W 态传输 1 比特经典信息。

虽然 QSDC 协议无需事先生成密钥,但基于 W 态的 QSDC 协议效率都不高,此外,基于 W 态的 QIS 方案还比较少。为此,提出了一种基于 W 态的量子信息拆分方案,方案中 1 个 W 态可直接共享 2 比特的经典信息,效率比较高,量子比特效率达到了 67%,并且可以很好地阻止外部窃听和防止内部不诚实参与者的欺骗,在理论上是安全的。

1 基于经典比特的量子信息拆分

1.1 相关知识与符号描述

本文方案主要是基于 W 态和局域操作实现秘密拆分的。一个 3 粒子 W 态是一个纠缠态,3 个粒子之间的关系存在关联,即一个粒子的状态改变会影响到其他粒子的状态改变。3 粒子W 态的标准形式[9]如下:

$$|w\rangle = \sqrt{a}|001\rangle + \sqrt{b}|010\rangle + \sqrt{c}|100\rangle + \sqrt{d}|000\rangle$$

其中:$a,b,c>0$;$d=1-(a+b+c)\geqslant 0$。协议中涉及的 W 态为 $|w\rangle = 1/2(|100\rangle + |010\rangle + \sqrt{2}|001\rangle)$,以及 4 个正交类 W 态:

$$|w_1\rangle = \frac{1}{2}(|000\rangle + |110\rangle + \sqrt{2}|101\rangle)$$

$$|w_2\rangle = \frac{1}{2}(|000\rangle + |110\rangle - \sqrt{2}|101\rangle)$$

$$|w_3\rangle = \frac{1}{2}(|001\rangle + |111\rangle + \sqrt{2}|100\rangle)$$

$$|w_4\rangle = \frac{1}{2}(|001\rangle + |111\rangle - \sqrt{2}|100\rangle)$$

4 个局域操作为:

$$U_1 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$$

$$U_2 = \sigma_Z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

$$U_3 = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$U_4 = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$$

对粒子进行局域操作会使粒子状态发生变化,如对 $|w\rangle$ 态中的第一个粒子进行 U_3 操作,$|w\rangle$ 态将变为 $|w_1\rangle$ 态。同时,Alice、Bob 和 Charlie 事先约定好 U_1、U_2、U_3、U_4 操作分表代表 00,01,10,11 比特。

1.2 方案的描述

假设 Alice 是秘密的分发者,她有 $M=2N$ 比特秘密信息,要发送给 Bob 和 Charlie,使得 Bob 和 Charlie 不能单独得到秘密,只有一起合作才能获得秘密。要达到这个目的,可通过以下 5 步来实现(方案原理如图 1 所示):

1)Alice 产生一组形如

$$|w\rangle = \frac{1}{2}(|100\rangle + |010\rangle + \sqrt{2}|001\rangle)$$

的 W 态,并将其分为 3 个序列:第一个粒子组成序列 S_1,第二个粒子组成序列 S_2,第三个粒子组成序列 S_3。同时,Alice 生成一组非正交态粒子,每个粒子随机处于 4 个态{$|0\rangle$,$|1\rangle$,$|+\rangle$,$|-\rangle$}之一,把这些非正交态粒子随机插入序列 S_2 中(注意只有 Alice 知道这些非正交态粒子的位置和状态),得到的新粒子序列记为 S_2',将 S_2' 发送给 Bob。

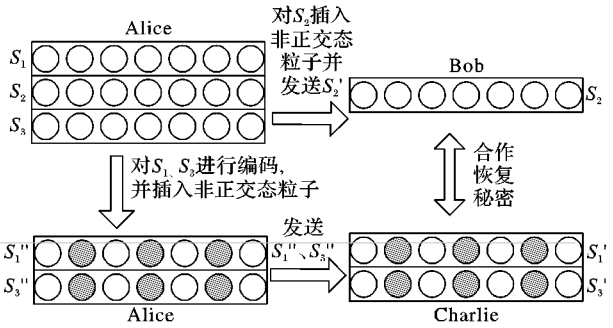

图 1 基于 W 态的 QIS 协议

2)Alice 与 Bob 进行检测窃听:Bob 收到 S_2' 后,通过公开信道告知 Alice,Alice 声明插入的非正交态粒子的位置和基信息,根据 Alice 的声明,Bob 从 S_2' 中选出这些非正交态粒子并用相应的基测量,这样 Alice 就可以通过比较初始态和测量结果来检测窃听,如果错误率低于某个特定的阈值,则认为信道中不存在窃听;反之,则认为存在窃听并停止本次通信。检测窃听完后,Bob 获得粒子序列 S_2。

3)Alice 对 S_1、S_3 序列中的粒子分别进行编码:先对 S_1 中的粒子进行 U_3 操作得到 S_1',若秘密消息 M 中的比特分别为 00,01,10 或 11,则对 S_3 中的粒子分别做 U_1、U_2、U_3、U_4 操作,得到 S_3'。Alice 生成一组非正交态粒子,每个粒子随机处于 4 个态{$|0\rangle$,$|1\rangle$,$|+\rangle$,$|-\rangle$}之一,把这些非正交态粒子分别随机插入编码后的 S_1'、S_3' 中,同样,只有 Alice 知道这些非正

交态粒子的位置和状态,得到的新粒子序列记为 S_1''、S_3'',把 S_1''、S_3'' 分别发送给 Charlie。

4) Alice 与 Charlie 采用第 2) 步的方法进行检测窃听:Charlie 收到 S_1''、S_3'' 后,通过公开信道告知 Alice,然后 Alice 声明插入的非正交态粒子的位置和基信息,根据 Alice 的声明,Charlie 从 S_1''、S_3'' 中选出这些非正交态粒子并用相应的基测量。这样 Alice 就可以通过比较初始态和测量结果来检测窃听,如果错误率低于某个特定的阈值,则认为信道中不存在窃听;反之,则认为存在窃听并停止本次通信,检测窃听完后,Charlie 获得编码后的粒子序列 S_1'、S_3'。

5) 当 Bob 和 Charlie 想要获得 Alice 的信息时,使用正交基 $|w_1\rangle$、$|w_2\rangle$、$|w_3\rangle$、$|w_4\rangle$,提供他们各自手中的粒子 S_2 和 S_1'、S_3',进行三粒子投影测量,根据三粒子之间的关联如表 1,就可获得 Alice 的原始秘密 M。

表 1　局域操作与三粒子投影测量结果之间的联系

Alice 局域操作	投影测量结果
$U_3 \otimes U_1 \otimes U_1$	$\|w_1\rangle$
$U_3 \otimes U_1 \otimes U_2$	$\|w_2\rangle$
$U_3 \otimes U_1 \otimes U_3$	$\|w_3\rangle$
$U_3 \otimes U_1 \otimes U_4$	$\|w_4\rangle$

例如 Alice 要共享的秘密信息为 $M = 00110110$,将序列分解成 $M = 00,11,01,10$,她先对序列 S_1 利用 U_3 操作进行编码,再对序列 S_3 利用 U_1、U_4、U_2、U_3 操作进行编码,进而得到 S_1'、S_3' 发送给 Charlie,给 Bob 的 S_2 不做变化,操作完成后的量子态转换成 $|w_1\rangle$、$|w_4\rangle$、$|w_2\rangle$、$|w_3\rangle$;当 Bob 和 Charlie 合作恢复 Alice 的秘密时,如果不存在窃听,他们的投影测量结果必为 $|w_1\rangle$、$|w_4\rangle$、$|w_2\rangle$、$|w_3\rangle$,从而推出 Alice 对序列 S_3 所做的操作,即恢复了原始秘密信息 M。

2　安全性分析

假设存在窃听者 Eve,她的目的是获得 Alice 的秘密信息,并不被检测到。下面通过分析来说明,这是不可能实现的。事实上,就窃听而言,参与者 Bob 和 Charlie 往往比外部窃听者具有更强的窃听能力,因为他们拥有部分秘密信息,并且在检测测听过程中有条件通过公布虚假信息来掩盖自己的窃听行为[26]。可以这样认为,在一个 QIS 方案中如果所有参与者都不能成功欺骗,那么 Eve 的窃听行为同样不能成功,从而说明协议是安全的。因此,下面针对 Bob 不诚实(记为 Bob*)的情况,考虑几种最常用的攻击手段-截获-测量(Intercept-and-Measure)、截获-重发(Intercept-and-Resend)和纠缠附加粒子(Entangled ancillary particles),来分析方案的安全性。对于 Charlie 不诚实的情况,也是一样的分析。

2.1　截获-测量攻击

截获-测量是指截获合法粒子并用相应的基进行测量,或将截获的粒子与手中的粒子作联合投影测量,测量完成后再将截获的粒子发送给合法通信者。具体为,Bob* 截获 Alice 发给 Charlie 的粒子 S_1''、S_3'',对 S_1''、S_3'' 和自己手中的 S_2 作投影测量,之后把 S_1''、S_3'' 重新发给 Bob。他的目的是得到 Alice 的秘密,即 3 粒子投影测量结果,但这种策略不会成功,因为 S_1''、S_3'' 中粒子的位置已经被 Alice 插入的非正交态粒子打乱,Bob* 不能确定哪三个粒子最初处于一个纠缠态,因此这种攻击方式不会成功。同样如果 Charlie 不诚实,她截获到的粒子序列只能是 Alice 随机插入非正交态后的 S_2' 序列,而非 S_2 序列,所以这种攻击方式对于不诚实的 Charlie 也不会成功。

2.2　截获-重发攻击

截获-重发是指 Bob* 截获合法粒子并用假冒粒子替换掉,具体为 Bob* 产生同样形式的 W 态 $|w\rangle = 1/2(|100\rangle + |010\rangle + \sqrt{2}|001\rangle)$,并截获 Alice 发给 Charlie 的 S_1''、S_3'',然后从制备的假粒子态中选择第 1,3 个粒子发给 Charlie,保留另一个粒子,这样 Bob* 可以在 Alice 公布非正交态粒子的位置后扔掉它们,并用 3 粒子投影测量 S_1''、S_3'' 中剩余的粒子(即为 Alice 编码好的 S_1'、S_3')和自己手中的粒子 S_2,进而得到 Alice 的秘密。但由于 S_1''、S_3'' 序列中的非正交态粒子是随机插入的,Bob* 发送假冒粒子时不知道非正交态粒子的位置和状态,对于 Bob* 发送的假冒粒子,每个粒子通过检测窃听的概率是 3/4(与 BB84 协议一样),因此不管 Bob* 准备什么样的粒子序列发给 Charlie,都将在第 4) 步 Alice 与 Charlie 检测窃听时,以 $1-(3/4)^l$(l 为 Alice 插入的非正交态粒子的数量)的概率被检测到,所以这种攻击方式也不会成功。若不诚实的 Charlie 采用这种攻击策略,也将以 $1-(3/4))^l$ 的概率被检测到。

2.3　纠缠附加粒子攻击

Bob* 的另一种攻击策略是纠缠附加粒子攻击[12]。具体为,Bob* 通过一个局域酉操作 $\hat{U}$ 把准备好的附加粒子 $|E\rangle = \{|E_1\rangle, |E_2\rangle, \cdots, |E_k\rangle\}$ 纠缠进 Alice 发给 Charlie 的粒子序列 S_1''、S_3'' 中,并在接下来的某个时间通过测量附加粒子得到关于 Charlie 的秘密信息。事实上,这种攻击策略也是无效的。

要想不被发现,Bob* 作用在非正交态粒子和附加粒子上的局域酉操作 $\hat{U}$ 需要满足如下条件:

$$\hat{U}|0\rangle|E_i\rangle = a|0\rangle|\delta_{00}\rangle + b|1\rangle|\delta_{01}\rangle = a|0\rangle|\delta_{00}\rangle \tag{1}$$

$$\hat{U}|1\rangle|E_i\rangle = c|0\rangle|\delta_{10}\rangle + d|1\rangle|\delta_{11}\rangle = d|1\rangle|\delta_{11}\rangle \tag{2}$$

$$\begin{aligned}\hat{U}|+\rangle|E_i\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle|\delta_{00}\rangle + b|1\rangle|\delta_{01}\rangle + c|0\rangle|\delta_{10}\rangle + d|1\rangle|\delta_{11}\rangle) = \\ &\frac{1}{2}[|+\rangle(a|\delta_{00}\rangle + b|\delta_{01}\rangle + c|\delta_{10}\rangle + d|\delta_{11}\rangle) + \\ &|-\rangle(a|\delta_{00}\rangle - b|\delta_{01}\rangle + c|\delta_{10}\rangle - d|\delta_{11}\rangle)] = \\ &\frac{1}{2}|+\rangle(a|\delta_{00}\rangle + b|\delta_{01}\rangle + c|\delta_{10}\rangle + d|\delta_{11}\rangle)\end{aligned} \tag{3}$$

$$\begin{aligned}\hat{U}|-\rangle|E_i\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle|\delta_{00}\rangle + b|1\rangle|\delta_{01}\rangle - c|0\rangle|\delta_{10}\rangle - d|1\rangle|\delta_{11}\rangle) = \\ &\frac{1}{2}[|+\rangle(a|\delta_{00}\rangle + b|\delta_{01}\rangle - c|\delta_{10}\rangle - d|\delta_{11}\rangle) + \\ &|-\rangle(a|\delta_{00}\rangle - b|\delta_{01}\rangle - c|\delta_{10}\rangle + d|\delta_{11}\rangle)] = \\ &\frac{1}{2}|-\rangle(a|\delta_{00}\rangle - b|\delta_{01}\rangle - c|\delta_{10}\rangle + d|\delta_{11}\rangle)\end{aligned} \tag{4}$$

其中:$|E_i\rangle$ 是 Bob* 的附加粒子,$|\delta_{00}\rangle$、$|\delta_{01}\rangle$、$|\delta_{10}\rangle$、$|\delta_{11}\rangle$

是 Bob* 测量时可以区分的态，同时有 $|a|^2+|b|^2=1$，$|c|^2+|d|^2=1$。

由式(1) ~ (4) 可知：

$$\begin{cases} b=c=0 \\ a|\delta_{00}\rangle - b|\delta_{01}\rangle + c|\delta_{10}\rangle - d|\delta_{11}\rangle = 0 \\ a|\delta_{00}\rangle + b|\delta_{01}\rangle - c|\delta_{10}\rangle - d|\delta_{11}\rangle = 0 \end{cases}$$

于是，$a|\delta_{00}\rangle = d|\delta_{11}\rangle$，即 Bob* 不能区分 $a|\delta_{00}\rangle$ 与 $d|\delta_{11}\rangle$，因此 Bob* 不能通过测量附加粒子来获得 Charlie 的信息。

综上所述，本文提出的量子信息拆分方案是安全的，既可以有效抵抗截获-测量与截获-重发的攻击策略，也可以抵抗纠缠附加粒子的窃听攻击。

3 效率分析

除了具有较良好的安全性，本文方案与其他基于 W 态的 QSDC 方案相比还具有较高的效率。为方便比较，假设各方案中要共享的秘密比特数均为 $2k$，下面从方案所需的粒子总数和量子比特效率两方面进行比较。根据量子比特效率[27]的定义为：

$$\eta_q = q_u/q_t$$

其中：q_u 表示最终有效的量子比特数目，q_t 表示的是通过量子信道传输的比特总数。

在文献[21]中，1个4粒子W态传送1个经典比特信息，要共享 $2k$ 比特信息，需要 $2k$ 个 W 态，$8k$ 个粒子，效率为 $2k/8k=25\%$；文献[22]中1个3粒子 W 态以2/3概率传送1比特信息，共享 $2k$ 比特信息，需要 $3k$ 个W态，$9k$ 个粒子，效率为 $(2/3)\times(2k/6k)\approx 22\%$；文献[23]中借助一个辅助粒子实现1个3粒子W态传送1比特信息，共享 $2k$ 比特信息，共需要 $6k$ 个粒子，效率为 $2k/6k\approx 33\%$；文献[24 - 25]实现1个3粒子W态传送1比特信息，共享 $2k$ 比特信息，共需要 $6k$ 个粒子，效率为 $2k/6k\approx 33\%$。

本文方案中，除了插入的非正交态粒子，每个 W 态都能在 Alice、Bob 和 Charlie 之间生成2比特经典秘密信息，所以要共享 $2k$ 比特的经典秘密，总共需要 k 个 W 态，即 $3k$ 个粒子，在理论上量子比特效率 $\eta_q = 2k/3k\approx 67\%$。本文方案与其他方案的效率对比如表2所示。

表2 本文方案与其他方案的效率对比

方案	粒子总数	效率/%
文献[21]方案	$8k$	25
文献[22]方案	$9k$	22
文献[23]方案	$6k$	33
文献[24 - 25]方案	$6k$	33
本文方案	$3k$	67

4 结语

本文利用 QSDC 和密集编码的思想提出了一个基于 W 态的高效量子信息拆分方案。方案中通信用户不再需要事先建立会话密钥，借助量子信道，Alice 直接让 Bob 和 Charlie 共享其秘密消息，比以往的量子信息拆分方案更为简单，分析表明该方案是安全的。方案在提高安全性的同时，还具备高效率的特点，量子比特效率达到67%，并且只需要一次代价较高的量子通信，其他通信则由代价较低的经典信道完成；另外方案中所涉及的量子态与局域操作在目前实验条件下均不难实现，因此具有较高的可行性。

参考文献：

[1] CLEVE R, GOTTESMAN D, LO H K. How to share a quantum secret [J]. Physical Review Letters, 1999, 83(3): 648 - 651.

[2] BENNET C H, BRASSARD G. Quantum cryptography: public-key distribution and coin tossing [C]// Proceedings of the 1984 IEEE International Conference on Computers, Systems and Signal Processing. Piscataway: IEEE Press, 1984: 175 - 179.

[3] BOSTROM K, FELBINGER T. Deterministic secure direct communication using entanglement[J]. Physical Review Letters, 2002, 89(18): 187902.

[4] ZENG G, ZHANG W. Identity verification in quantum distribution [J]. Physical Review A, 2000, 61(2): 022301 - 022303.

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

[6] BAGHERINEZHAD S, KARIMIPOUR V. Quantum secret sharing based on reusable Greenberger-Horne-Zeilinger states as secure carriers [J]. Physical Review A, 2003, 67(4): 044302.

[7] XIE D, YE M, LI X. Improved multipartite quantum secret sharing protocol using preshared Greenberger-Horne-Zeilinger states [J]. Communications in Theoretical Physics, 2011, 56(6): 1027 - 1030.

[8] DENG F, LONG G, ZHOU H. An efficient quantum secret sharing scheme with Einstein-Podolsky-Rosen pairs [J]. Physics Letters A, 2005, 340(1): 43 - 50.

[9] DÜR W, VIDAL G, CIRAC J I. Three qubits can be entangled in two inequivalent ways [J]. Physical Review A, 2000, 62(6): 062314.

[10] AGRAWAL P, PATI A. Perfect teleportation and superdense coding with W states [J]. Physical Review A, 2006, 74(6): 062320.

[11] LI L, QIU D. The states of W-class as shared resources for perfect teleportation and superdense coding [J]. Physics A: Mathematical and Theoretical, 2007, 40(35): 10871.

[12] HWANG T, HWANG C C, LI C M. Multiparty quantum secret sharing based on GHZ states [J]. Physica Scripta, 2011, 83(4): 045004.

[13] LIU X, PAN R. Cryptanalysis of quantum secret sharing based on GHZ states [J]. Physica Scripta, 2011, 84(4): 045015.

[14] TAN X, JIANG L. Improved three-party quantum secret sharing based on Bell states [J]. International Journal of Theoretical Physics, 2013, 52(10): 3577 - 3585.

[15] CURTY M, LÜTKENHAUS N. Intercept-resend attacks in the Bennett-Brassard 1984 quantum-key-distribution protocol with weak coherent pulses [J]. Physical Review A, 2005, 71(6): 1 - 10.

[16] YANG C W, TSAI C W, HWANG T. Thwarting intercept-and-resend attack on Zhang's quantum secret sharing using collective rotation noises [J]. Quantum Information Processing, 2012, 11(1): 113 - 122.

[17] ZHANG B, LIU Y. A postselection-based linear optical scheme for generation of a three-photon W state [J]. Journal of Physics B: Atomic, Molecular and Optical Physics, 2009, 42(19): 195504.

[18] CARDOSO W B, QIANG W C, AVELAR A T, *et al.* Generation of two-photon EPR and W states [J]. Journal of Physics B: Atomic, Molecular and Optical Physics, 2010, 43(15): 155502.

(下转第995页)

$L_2 \times f_2 = 3.257$ Gb/s。

设 $n = 10000$,即完成 10000 组数据操作,非流水线实现方式需要的时间为 7 730 μs,而流水线方式需要的时间为 1 573 μs。因此,流水线实现方式对于大规模报文的运算处理更加高效,适合于网络处理器加密引擎。

通过实验分析,在使用 GX EP2AGX125 器件的情况下,非流水线方式能够达到的最高频率 $f_1 = 87.969$ MHz,最大数据吞吐率为 662.354 Mb/s;而流水线方式的最高频率 $f_2 = 114.499$ MHz,最大数据吞吐率为 3.257 Gb/s。如果完成 10000组数据操作,非流水线实现方式需要的时间为7 730 μs,而流水线方式需要的时间为 1 573 μs,当 n 足够大时,MD5 流水线硬件实现使运算速度提高近 5 倍,而且消耗的资源相对不大,完全可以接受。因此,MD5 算法流水线硬件加速模型更加高效。

5　结语

本文基于开发验证平台 NetMagic 实现了 MD5 硬件加速算法,并对其功能模块进行了仿真验证和性能测试。实验结果表明,MD5 硬件加速算法能够快速计算出数据的摘要信息,对于大规模流量的报文,在处理速度方面,加速比趋近于 5,而且在处理速度提高的同时,其资源消耗并未明显增加。因此可以证明该模型可有效用于超高吞吐量报文处理和大量短报文 MD5 值的暴力破解,处理效率高,而且成本较低,较其他实现方式更具优越性和应用前景。

参考文献:

[1] RIVEST R. RFC1321, the MD5 message-digest algorithm[S]. Geneva: IETF, 1992.

[2] JARVINEN K, TOMMISKA M, SKYTTA J. Hardware implementation analysis of the MD5 Hash algorithm[C]// Proceedings of the 38th Annual Hawaii International Conference on System Sciences. Piscataway: IEEE Press, 2005: 298a.

[3] HONG Q, ZHOU Q, WANG Y, *et al*. Research and hardware realization of MD5 algorithm based on Hash function[J]. Computer Engineering, 2013, 39(3): 137 - 141. (洪琪, 周琴琴, 王永亮, 等. 基于 Hash 函数的 MD5 算法研究和硬件实现[J]. 计算机工程, 2013, 39(3): 137 - 141).

[4] CHEN S, HUANG W. FPGA Implementation of MD5 algorithm[J]. Information Security and Communications Privacy, 2007(6): 129 - 130. (陈松, 黄炜. MD5 算法的 FPGA 实现[J]. 信息安全与通信保密, 2007(6): 129 - 130.)

[5] LIU K, CHE M, QIN C. A high throughput FPGA implementation of MD5 algorithm[J]. Microprocessors, 2008, 29(1): 188 - 191. (刘凯, 车明, 秦存秀. 一种高吞吐量 MD5 算法的 FPGA 实现[J]. 微处理机, 2008, 29(1): 189 - 190.)

[6] MAO X, LI T, SUN Z. NetMagic innovative experimental platform design guide[M]. Changsha: National Defense University Press, 2012: 23 - 52. (毛席龙, 李韬, 孙志刚. NetMagic 创新实验平台设计指南[M]. 长沙: 国防科技大学出版社, 2012: 23 - 52.)

[7] SU Q, CHEN Y, JIA C, *et al*. Design and implementation of access and control method for NetMagic[C]// Proceedings of the 2011 International Conference on Mechatronic Science, Electric Engineering and Computer. Piscataway: IEEE Press, 2011: 346 - 349.

[8] NetMagic. How to develop NetMagic rapidly[EB/OL]. [2014-05-10]. http://www.netmagic.org/Netmagic_specification&whitepapers/Startup_How%20to%20Develop%20NetMagic%20Rapidly.pdf. (NetMagic. 如何开发 NetMagic 平台[EB/OL]. [2014-05-10]. http://www.netmagic.org/Netmagic_specification&whitepapers/Startup_How%20to%20Develop%20NetMagic%20Rapidly.pdf.)

[9] WANG Y, ZHAO Q, JIANG L, *et al*. Ultra high throughput implementations for MD5 Hash algorithm on FPGA [C]// Proceedings of the Second International Conference on High Performance Computing and Applications, LNCS 5938. Berlin: Springer-Verlag, 2010: 435 - 440.

[10] LIU T, LOU X. FPGA digital electronic systems design and development examples navigation [M]. Beijing: Posts and Telecom Press, 2005: 84 - 126. (刘韬, 楼兴华. FPGA 数字电子系统设计与开发实例导航[M]. 北京: 人民邮电出版社, 2005: 84 - 126.)

[11] ZHOU R, SU L. Quartus II-based digital system Verilog HDL design example explanation[M]. Beijing: Publishing House of Electronics Industry, 2010: 23 - 89. (周润景, 苏良碧. 基于 Quartus II 的数字系统 Verilog HDL 设计实例详解[M]. 北京: 电子工业出版社, 2010: 23 - 89.)

(上接第 984 页)

[19] ZHA X, SONG H. Two schemes of remote preparation of a four-particle entangled W state via a six-qubit maximally entangled state [J]. Physica Scripta, 2011, 84(1): 015010.

[20] LIN Q. Efficient generation of multi-photon W state [J]. Science China: Physica, Mechanica and Astronomica, 2012, 42(1): 54 - 60. (林青. 多光子 W 态的高效制备[J]. 中国科学: 物理学、力学、天文学, 2012, 42(1): 54 - 60.)

[21] CAO H, SONG H. Quantum secure direct communication with W states [J]. Chinese Physical Letters, 2006, 23(2): 290 - 292.

[22] CAO H, SONG H. Quantum secure direct communication using a W state and teleportation [J]. Physica Scripta, 2006, 74(5): 572 - 575.

[23] DONG L, XIU X, CAO Y, *et al*. Quantum secure direct communication using W state [J]. Communication in Theoretical Physicss, 2008, 49(6): 1495 - 1498.

[24] DONG L, XIU X, CAO Y, *et al*. Quantum secure direct communication using a class of three-particle W state [J]. Communication in Theoretical Physicss, 2008, 50(2): 359 - 362.

[25] LIU C, GENG H, LIU W. Secure quantum communication protocol based on symmetric W state and identity authentication [J]. Journal of Computer Applications, 2014, 34(2): 438 - 441. (刘超, 耿焕同, 刘文杰. 基于对称 W 态和身份认证的安全量子通信协议[J]. 计算机应用, 2014, 34(2): 438 - 441.)

[26] QIN S, GAO F, WEN Q, *et al*. Improving the security of multiparty quantum secret sharing against an attack with a fake signal [J]. Physics Letters A, 2006, 357(2): 101 - 103.

[27] SUN Y, DU J, QIN S, *et al*. Two-way authentication quantum secret sharing [J]. Journal of Physics, 2008, 57(8): 4689 - 4694. (孙莹, 杜建忠, 秦素娟, 等. 具有双向认证功能的量子秘密共享方案[J]. 物理学报, 2008, 57(8): 4689 - 4694.)