互联网中任意终端间量子密钥中继协议*

徐人凤[1]，肖正兴[1]，李粤平[1,2]，聂 哲[1]，温晓军[1,3†]

(1. 深圳职业技术学院 计算机工程学院，广东 深圳 518055；2. 哈尔滨工业大学深圳研究生院，广东 深圳 518055；3. 北京交通大学 通信与信息系统北京市重点实验室，北京 100044)

摘 要：提出了量子密钥中继的概念及协议。利用量子纠缠特性或者量子隐形传态可以实现不相邻两台终端设备间共享量子密钥，即量子密钥中继，最终实现互联网中任意终端间的量子密钥共享，并具有无条件的安全性。

关键词：量子密钥中继；无条件安全性；互联网

中图分类号：TN918.91 **文献标志码**：A **文章编号**：1001-3695(2013)02-0507-03

doi:10.3969/j.issn.1001-3695.2013.02.052

Quantum key relay protocols between any terminals in Internet

XU Ren-feng[1], XIAO Zheng-xing[1], LI Yue-ping[1,2], NIE Zhe[1], WEN Xiao-jun[1,3†]

(1. *School of Computer Engineering, Shenzhen Polytechnic, Shenzhen Guangdong* 518055, *China*; 2. *Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen Guangdong* 518055, *China*; 3. *Key Laboratory of Communication & Information System, Beijing Jiaotong University, Beijing* 100044, *China*)

Abstract: This paper proposed the concepts and protocols of quantum key relay. Using quantum entanglement properties or quantum teleportation, quantum key sharing between the two non-adjacent terminal equipments can be achieved, i.e., quantum key relay, and ultimately achieve the quantum secret sharing between any terminals in the Internet, furthermore, they had the unconditional security.

Key words: quantum key relay; unconditional security; Internet

0 引言

互联网的出现，使人们切身体会到了信息革命带来的高效率和高效益，极大地推动了生产力的发展。然而，正如当今现实社会中与国际间存在着竞争、斗争、犯罪甚至战争一样，在互联网这个虚拟空间中同样也充斥着大量不文明和暴力行为。犯罪分子利用互联网自身安全的脆弱性，运用其“暴智”来实施虚拟空间的“暴力”犯罪行为，诸如散布计算机病毒、非法侵入他人系统、窥探个人隐私，甚至盗窃国家经济、军事情报，侵吞公私资产，以达到其贪婪的目的。因此，互联网的信息安全问题是至关重要的。目前担当为互联网安全保驾护航重任的就是基于数学计算复杂性的现代密码体制，然而它却面临着日益逼近的致命性威胁——量子计算机等即将成为现实的新型高性能计算机将攻破现有的绝大多数数学密码体制。

现代密码体制的安全性问题，从物理的角度来看，此种密码体制即使对简单的窃听攻击也无法检测，是其固有的第一大缺陷；从数学的角度来看，现代密码体制大多是基于计算复杂性设计密码算法，而随着计算能力的提高，这些算法很容易被攻破，量子计算机能在几秒钟内将著名的经典密码学算法如 RSA(Rivest-Shamir-Adleman)算法攻破。现已证明，除 RSA 外，量子 Shor 算法还可以轻易攻破常用的 DSA 和 ECDSA 等。特别是大量量子计算机组成分布式网络，其强大的计算能力是不可想象的，基于计算复杂性的现代密码体制的根基将被动摇。根据大多数学者公认的预测，在 2020 年左右，大型量子计算机可能会成功运行，到那时用于保护互联网中数据安全的所有现在的公钥密码算法都将会被攻破。

幸运的是，现代密码体制的上述两大缺陷被证明可以用量子密码技术来进行弥补，这是由量子密码的两个基本特征，即对窃听的可检测性和无条件安全性决定的[1,2]。因为量子密码的安全性由量子信息的物理特性来保证，而不是基于数学上的计算复杂性问题，因而与攻击者的计算能力或计算资源的大小无关，这种安全性通常称为量子密码的无条件安全性。另外，攻击者的行为必将对量子态产生扰动而被发现，这就是量子密码对窃听攻击的可检测性，这两种性质是经典密码所不具有的。

学术界已证明量子密钥分配(quantum key distribution, QKD)结合一次一密算法(one time pad)设计通信协议可以获得无条件安全性[3]。因此量子密钥分发与共享是量子保密通信网络系统的基础，也是各种量子保密通信高级协议中的关键步骤之一[4,5]。当前的量子保密技术与现有互联网相融合的研究主要是量子密钥分发网络结合经典通信技术而形成量子—经典混合式的安全互联网系统。目前任意终端间的密钥共享需要通过两种方式实现：a)量子方式，对于相邻的两台终端设备间共享密钥，量子密钥分发技术作为密钥分配方式；b)经典方式，对于不相邻的两台终端间共享密钥，根据应用需要采用经典可信中继(trusted relay)的方式。通过这两种方式可以实现系统中任意终端间的密钥共享。

收稿日期：2012-07-17；**修回日期**：2012-08-20 **基金项目**：国家自然科学基金资助项目(61100190)

作者简介：徐人凤(1961-)，女，辽宁沈阳人，高级工程师，主要研究方向为数据库应用、数据挖掘；肖正兴(1976-)，男，江西永新人，讲师，硕士，主要研究方向为人工智能；李粤平(1980-)，男，广东韶关人，讲师，博士，主要研究方向为网络计算；聂哲(1970-)，男，湖南益阳人，教授，硕士，主要研究方向为网络舆情；温晓军(1971-)，男(通信作者)，江西赣州人，教授，博士，主要研究方向为量子密码(szwxjun@sina.com).

显然利用可信中继无法达到无条件安全。本文提出了量子密钥中继的概念,从而对于情况 b)不必采用经典方式,利用量子密钥中继即可实现不相邻的两台终端间量子密钥的共享,以实现互联网通信的无条件安全。随着“光纤到户”的城市全光网络的飞速发展,以及量子信息技术进入实用化和产业化阶段,利用量子密钥中继可实现量子安全通信与互联网应用技术的融合,具有良好的应用前景,将带来显著的经济效益和社会效益。

1 基本原理

1.1 量子纠缠特性

以四维的复线性空间中的纠缠态为例来简要介绍量子纠缠态的概念[1]。设 V 和 W 均表示二维的复线性空间,基矢为 $\{|0\rangle,|1\rangle\}$,则由 V 和 W 张量积组成四维的复线性空间 $V\otimes W$,其基矢为 $\{|00\rangle,|10\rangle,|01\rangle,|11\rangle\}$。若 $V\otimes W$ 中态矢 $|\psi\rangle$ 满足

$$|\psi\neq|\psi\rangle\otimes|\phi\rangle \tag{1}$$

即 $|\psi\rangle$ 无法表示成二维的复线性空间 V 和 W 中的态矢 $|\psi\rangle$ 和 $|\phi\rangle$ 的直积,则称 $|\psi\rangle$ 为纠缠态(quantumentanglement state)。例如,量子态:

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2+|1\rangle_1|1\rangle_2) \tag{2}$$

就是一个纠缠态。当 $|\psi\rangle=|00\rangle$ 时表示第 1 个量子位和第 2 个量子位同时为 $|0\rangle$,$|\psi\rangle=|11\rangle$ 时则表示第 1 个量子位和第 2 个量子位同时为 $|1\rangle$,第 1 个量子位总是与第 2 个量子位纠缠在一起。为了表述方便,常略去下标,将式(2)简略表示为

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) \tag{3}$$

数学上可以证明式(3)表示的量子态 $|\psi\rangle$ 是纠缠的,现简略证明如下。假设 $|00\rangle+|11\rangle$ 能用两个独立的量子态的直积来描述,则必须找到四个复数 α、β、γ、δ 使它们满足

$$(\alpha|0\rangle+\beta|1\rangle)\otimes(\gamma|0\rangle+\delta|1\rangle)=|00\rangle+|11\rangle \tag{4}$$

由于

$$(\alpha|0\rangle+\beta|1\rangle)\otimes(\gamma|0\rangle+\delta|1\rangle)=\alpha\gamma|00\rangle+\alpha\delta|01\rangle+\beta\gamma|10\rangle+\beta\delta|11\rangle \tag{5}$$

如果要使式(4)成立,由式(5)知其充要条件为 $\alpha\gamma=\beta\delta=1$ 且 $\alpha\delta=\beta\gamma=0$,显然满足这个条件的四个复数 α、β、γ、δ 是不存在的。

常见纠缠态——Bell 态是指下面四个纠缠态:

$$|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) \tag{6}$$

$$|\Phi^-\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle) \tag{7}$$

$$|\Psi^+\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle) \tag{8}$$

$$|\Psi^-\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle) \tag{9}$$

处于 Bell 态的纠缠双粒子又称为 EPR(Einstein-Padolsky-Rosen)对,Bell 态在量子保密通信中起着非常重要的作用[6]。

1.2 量子隐形传态

量子隐形传态[7](quantum teleportation)的基本思想是:为实现传送光子 1 的未知量子态 $|\psi\rangle_1$,可将该光子的信息分成经典信息和量子信息并分别通过经典信道和量子信道传送给遥远的接收方。经典信息是发送者通过测量得到,而量子信息则是由 EPR 对的纠缠特性产生。接收者根据这两种信息,可以将原来要传送的光子 1 的量子态 $|\psi\rangle_1$ 在自己手上的另一个光子上恢复出来,同时在发送者手上原光子 1 的量子态因测量被破坏掉了。下面来具体描述量子隐形传态的过程。设 Alice 手中的光子 1 处于待传送的量子态:

$$|\psi\rangle_1=a|0\rangle+b|1\rangle \tag{10}$$

她同时制备由光子 2 和 3 组成的 EPR 纠缠态:

$$|\Psi^-\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle) \tag{11}$$

Alice 留下光子 2 在自己手中,把光子 3 发送给远处的 Bob,此时三个光子的混合态表示为

$$|\psi\rangle_{123}=\frac{1}{2}[|\Psi^-\rangle_{12}(-a|0\rangle-b|1\rangle)_3+|\Psi^+\rangle_{12}(-a|0\rangle+b|1\rangle)_3+|\Phi^-\rangle_{12}(b|0\rangle+a|1\rangle)_3+|\Phi^+\rangle_{12}(-b|0\rangle+a|1\rangle)_3] \tag{12}$$

Alice 对光子 1、2 用 Bell 基进行测量,并公开她的测量结果。根据式(12),Bob 手中的光子 3 将在 Alice 测量后的瞬间塌缩到相应的量子态,于是 Bob 采用相应的量子变换可以将光子 3 恢复到与光子 1 的初态 $|\psi\rangle_1$ 相同的态。

例如,假定 Alice 对光子 1、2 测量结果为 $|\Psi^-|_{12}$,则 Bob 手中的光子 3 将塌缩到 $-a|0\rangle-b|1\rangle$,Bob 对其作如下变换即可恢复光子 1 的初态 $a|0\rangle+b|1\rangle$:

$$U=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} \tag{13}$$

其他情况如表 1 所示。

表 1 量子隐形传态中的量子操作

Alice 对光子 1,2 的测量结果	Bob 手中光子 3 的状态	Bob 恢复量子态的操作	Alice 对光子 1,2 的测量结果	Bob 手中光子 3 的状态	Bob 恢复量子态的操作
$\|\Psi^-\rangle_{12}$	$-a\|0\rangle-b\|1\rangle$	$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$	$\|\Phi^-\rangle_{122}$	$b\|0\rangle+a\|1\rangle$	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
$\|\Psi^+\rangle_{12}$	$-a\|0\rangle+b\|1\rangle$	$\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}$	$\|\Phi^+\rangle_{12}$	$-b\|0\rangle+a\|1\rangle$	$\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$

2 量子密钥中继协议

相邻的两台终端设备间共享密钥,可通过量子密钥分发如著名的 BB84 协议作为无条件安全的密钥分配方式来实现。非相邻的两台终端设备间共享密钥,目前普遍采用经典可信中继的方式,然而不能保证其无条件安全性。因此,本文提出了下面两种量子中继方式。

2.1 利用 Bell 纠缠态实现量子密钥中继

设终端 Alice 和 Bob 是相邻的,两者可以通过上述 QKD 协议实现密钥共享。终端 Charlie 是与终端 Alice 不相邻的,但他与 Bob 是相邻的,Charlie 可以通过 Bob 作为中继与 Alice 实现密钥共享。

首先,Alice 和 Bob 通过 BB84 等 QKD 协议实现密钥共享,Bob 得到 Alice 的原始密钥 $K=\{m(1),m(2),\cdots,m(i),\cdots,m(M)\}$(二进制序列),其中 $m(i)\in\{0,1\}$。Bob 为将此密钥中继给远方的 Charlie,须作如下操作:

a)Bob 制备量子信道。他制备 M' 组($M'>M$)如式(6)所示的 EPR 纠缠对光子 $|\psi(i)\rangle_{12}(i=1,2,\cdots,M,\cdots,M')$,易知,该纠缠态在基 B_X 下也可以表示为

$$|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|++\rangle+|--\rangle) \tag{14}$$

对于每对光子,Bob 留下光子 1,光子 2 则发送给 Charlie,

如图 1 所示。

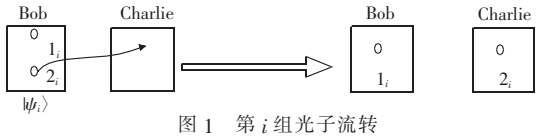


图 1　第 i 组光子流转

b)量子信道安全性检测。为了防止截断/重发攻击或中间人攻击,需首先对量子信道安全性进行检测。Bob 从自己留下的光子 1 序列中随机挑选($M'-M$)个光子,并随机以基 B_Z 或 B_X 进行测量,然后向 Charlie 宣布这些光子在序列中的编号和测量基。由式(6)(14)可知,如果没有攻击存在,若 Bob 的测量结果为$|0\rangle$态,则 Charlie 手上对应的光子 2 的量子态也必然塌缩为$|0\rangle$态;若 Bob 对光子 1 的测量结果为$|1\rangle$态,则光子 2 的量子态也必然为$|1\rangle$态;若 Bob 对光子 1 的测量结果为$|+\rangle$态,则光子 2 的量子态也必然为$|+\rangle$态;若 Bob 对光子 1 的测量结果为$|-\rangle$态,则光子 2 的量子态也必然为$|-\rangle$态。接到 Bob 的通知后, Charlie 按照正确的测量基依次测量自己手上对应编号的光子 2 的量子态。双方公开比较测量结果,若测量结果符合上述规律,则表明信道是安全的,剩余的 N 组 EPR 纠缠态光子用于量子密钥的中继。

c)Bob 根据原始密钥按照下面的测量规则随机使用基 B_Z 或 B_X 选择 $+z(+x)$或 $-z(-x)$方向测量自己手中的光子 1 序列。

$$\text{Bob 测量方向}=\begin{cases}+z(+x) & m(i)=0\\ -z(-x) & m(i)=1\end{cases} \tag{15}$$

d)Bob 在测量后,仅通知 Charlie 随机选用的测量基即可。Charlie 采用同样的基测量自己手中的光子 2 序列的量子态$|\psi(i)\rangle_2$,测量结果按照下面的规则记录为二进制代码 $K'=\{m'(1),m'(2),\cdots,m'(i),\cdots,m'(M)\}$:

$$m'(i)=\begin{cases}0 & |\psi(i)\rangle_2=|+z\rangle\text{或}|+x\rangle\\ 1 & |\psi(i)\rangle_2=|-z\rangle\text{或}|-x\rangle\end{cases} \tag{16}$$

则 K'就是 Alice 要和 Charlie 共享的原始密钥,且 $K'=K$。

2.2　利用量子隐形传态实现量子密钥中继

2.1 节所述量子密钥中继协议中, Alice 和 Charlie 的共享密钥需要让 Bob 知道,而借助隐形传态的方法,可以使 Bob 承担中继而无法知道 Alice 与 Charlie 之间的密钥。具体协议如下:

a)Alice 按照 BB84 协议向 Bob 发送单光子序列。

b)设 Bob 从 Alice 处收到光子序列后,从中随机抽取部分光子进行窃听检测(检测窃听的方法参考 BB84 协议),确认无窃听后最终留下 M 个光子序列,记为光子 1 序列。设其中第 i 个光子的量子态为$|\psi_i\rangle_1$,如式(10)所示。

c)Bob 制备 M'组($M'>M$)如式(11)所示的包含光子 2、3 的 EPR 纠缠对,将每一对中光子 3 发送给远方的 Charlie,自己留下光子 2。光子流转如图 2 所示。同时按照 2.1 节中步骤 b)所述方法检测窃听,最终留下 M 对光子进行通信。

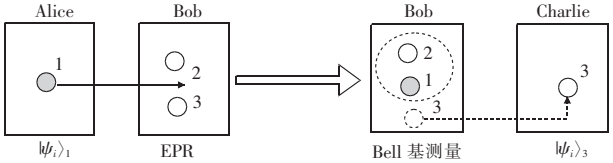


图 2　第 i 组光子的传递、Bell 基测量与隐形传态

d)按照 1.2 节中所述的量子隐形传态过程,将光子 1 序列第 i 个光子的量子态$|\psi_i\rangle$隐形传送到 Charlie 手中的光子 3 上。Charlie 将光子 3 序列按表 1 规则恢复出量子态$|\psi_i\rangle_3$。

e)此时由于$|\psi_i\rangle_1=|\psi_i\rangle_3$,Alice 可以和 Charlie 借鉴 BB84 的方法共享量子密钥。

3　安全性分析

本文中 2.1 节相邻终端 Alice 与 Bob 间密钥分发以及 2.2 节步骤 a)均采用 BB84 等 QKD 协议进行。这类协议已经被证明是无条件安全的。

在本文的两个量子中继协议中,均设置了有效的量子信道安全检测步骤,如 2.1 和 2.2 节的步骤 b)所述。因此,攻击者 Eve 的截获/重发、中间人等攻击方式是无法得逞的。假设 Eve 试图通过截获 EPR 对中的一个光子,测量它得到有用信息,然后将它或一个替代光子再重新发送给接收者,这样的做法是徒劳的。因为 Eve 不知道发送者采用的是哪种测量基,凭猜测她将有一半的测量基是错误的,因而她的测量不仅得不到任何有用信息,而且会破坏 EPR 纠缠对的相干性而被检测出来。

在 2.1 节协议中,需要中继 Bob 是可信的。而在 2.2 节协议中,可以不需要 Bob 是值得信赖的,Bob 虽然作为中继但也无从得知 Alice 和 Charlie 的共享密钥。因为在隐形传态前,Bob 拥有光子 1 序列,但他不能测量(他不知道测量基,测量会导致量子态的破坏);而一旦进行隐形传态后,光子 1 的量子态传递给光子 3,而光子 1 的量子态在隐形传态后被破坏掉了,因此 Bob 同样无法得知密钥的信息。

假设不诚实的 Bob 采用纠缠/测量的攻击方式来窃取 Alice 和 Charlie 的共享密钥,但这也是要失败的。分析如下:设 Bob 将一个处于态$|0\rangle$的附加光子 g 通过 CNOT 操作与他手上的光子 1 发生纠缠,然后再将操作后光子 1 的态按协议步骤隐形传递给光子 3,企图通过测量附加光子 g 来达到目的。但这样对纠缠粒子的测量不仅会破坏光子 1 的态,而且由于得不到 Charlie 正确的测量基,Bob 对附加光子的测量是毫无意义的。

可见,本文提出的量子中继协议对截获/重发、中间人或纠缠/测量等常见攻击方式都是安全的。

4　结束语

密钥分发与共享是各种安全协议中的关键步骤之一,也是互联网系统安全的基石。鉴于量子保密通信技术的无条件安全性,它将成为下一代安全通信的重要发展方向。当前的技术局限于采用量子密钥分发实现相邻的两台终端设备间共享密钥。

为了以完全的量子方式实现任意终端间的密钥共享,本文提出了量子密钥中继的概念以及两个量子密钥中继协议:a)利用 EPR 量子纠缠态来实现,Bob 参与中继的同时也会知道密钥的内容;b)利用隐形传态来实现,作为中继的 Bob 无法知道他所传递的密钥信息,安全性更高,当然会付出更高的通信成本(因为需要更多的光子参与)。

采用量子密钥中继协议,可以使不相邻的两台终端间共享密钥,从而实现互联网中任意终端间的量子密钥共享。借助于量子密钥及量子加密算法[8],系统用户可以在任意终端间实现无安全的数据传输,包括量子保密电话、文件传输、文字聊天等业务[9]。随着城市全光网络的建成及量子信息技术的发展,网络安全面临的迫切问题将得到根本性解决。

(下转第 512 页)

待攻击的密文矩阵为

$$C' = \begin{pmatrix} 103 & 167 & 86 & 145 \\ 53 & 64 & 47 & 89 \\ 67 & 46 & 58 & 96 \\ 112 & 128 & 109 & 143 \end{pmatrix}$$

根据式(16)有

$$P'^{rc} = C' \oplus C_0 = \begin{pmatrix} 70 & 121 & 34 & 106 \\ 70 & 42 & 96 & 22 \\ 50 & 48 & 70 & 39 \\ 91 & 58 & 60 & 11 \end{pmatrix} \tag{19}$$

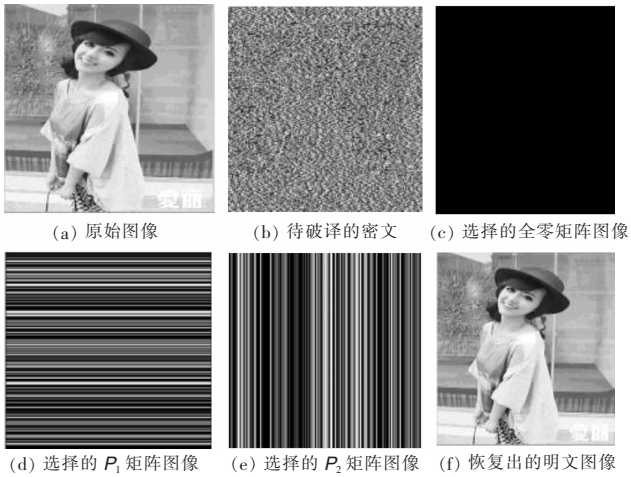
再根据式(17)可得

$P_1^c = C_1 \oplus C_0 = \begin{pmatrix} 5 & 6 & 4 & 3 \\ 5 & 6 & 4 & 3 \\ 5 & 6 & 4 & 3 \\ 5 & 6 & 4 & 3 \end{pmatrix}$，故可得到列变换系数 $c = \{3, 4, 2, 1\}$。利用列变换系数对行列置乱矩阵 P'^r 进行列反变换，即可得到 $P_1^{rc} = \begin{pmatrix} 34 & 106 & 121 & 70 \\ 96 & 22 & 42 & 70 \\ 70 & 39 & 48 & 50 \\ 60 & 11 & 58 & 91 \end{pmatrix}$。最后根据式(18)可得

$P_2^r = C_2 \oplus C_0 = \begin{pmatrix} 4 & 4 & 4 & 4 \\ 3 & 3 & 3 & 3 \\ 6 & 6 & 6 & 6 \\ 5 & 5 & 5 & 5 \end{pmatrix}$，故可得到行变换系数 $r = \{2, 1, 4, 3\}$。利用行变换系数对行置乱矩阵 P'^r 进行行反变换，即可得到 $P' = \begin{pmatrix} 96 & 22 & 42 & 70 \\ 34 & 106 & 121 & 70 \\ 60 & 11 & 58 & 91 \\ 70 & 39 & 48 & 50 \end{pmatrix}$。

4 仿真实验结果

以 256×256 灰度图像为例，图 1 给出了对 HYPER_HIE 算法进行选择明文攻击过程中的 MATLAB 仿真结果。



(a) 原始图像 (b) 待破译的密文 (c) 选择的全零矩阵图像

(d) 选择的 P_1 矩阵图像 (e) 选择的 P_2 矩阵图像 (f) 恢复出的明文图像

图 1 选择明文攻击过程中的 MATLAB 仿真结果

5 结束语

本文针对文献[5]的 HYPER_HIE 算法在安全性方面存在的问题，对其进行了选择明文攻击，整个攻击过程在未知密钥的前提下进行，结果以很小的计算代价对其密文进行了破译。在后续的研究中将对该算法进行改进。

参考文献：

[1] MATTHEWS R. On the derivation of a chaotic encryption algorithm [J]. Cryptologia, 1989, 13(1): 29-42.

[2] HEGAZI A S, MATOUK A E. Dynamical behaviors and synchronization in the fractional order hyperchaotic Chen system [J]. Applied Mathematics Letters, 2011, 24(11): 1938-1944.

[3] GAO Tie-gang, CHEN Zeng-qiang. A new image encryption algorithm based on hyper-chaos[J]. Physics Letters A, 2008, 372(4): 394-400.

[4] RHOUMA R, BELGHITH S. Cryptanalysis of a new image encryption algorithm based on hyper-chaos[J]. Physics Letters A, 2008, 372(38): 5973-5978.

[5] 王静, 蒋国平. 一种超混沌图像加密算法的安全性分析及其改进[J]. 物理学报, 2011, 60(6): 0605031-06050311.

[6] PARK J H. Adaptive synchronization of hyperchaotic Chen system with uncertain parameters[J]. Chaos, Solitons and Fractals, 2005, 26(3): 959-964.

[7] ZHANG Yu, LI Cheng-qing, LI Qin, *et al*. Breaking a chaotic image encryption algorithm based on perceptron model[J]. Nonlinear Dynamics, 2012, 69(3): 1091-1096.

[8] ZHAO Liang, ADHIKARI A, XIAO Di, *et al*. On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption[J]. Communication Nonlinear Science and Numerical Simulation, 2012, 17(8): 3303-3327.

(上接第 509 页)

参考文献：

[1] NIELSEN M, CHUANG I. Quantum computation and quantum information[M]. [S. l.]: Cambridge University Press, 2000.

[2] SCHIFF J, POIRIER B. Communication: quantum mechanics without wavefunctions[J]. Journal of Chemical Physics, 2012, 136(3): 031102-031105.

[3] LU Hua, FUNG C H F, MA Xiong-feng, *et al*. Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel [J]. Physical Review A, 2011, 84(4): 042344-042348.

[4] KHIRA M F A, ZAINC M N M, ISKANDAR B, *et al*. Implementation of two-way quantum key distribution protocol with decoy state[J]. Optics Communications, 2012, 285(5): 842-845.

[5] YANG Jing, WANG Chuan, ZHANG Ru. Quantum secure direct communication with authentication expansion using single photons[J]. Communications in Theoretical Physics, 2010, 54(5): 829-834.

[6] WANG Zhi-xi. Quantum secure direct communication and quantum sealed-bid auction with EPR pairs[J]. Communications Theoretical, Physics, 2010, 54(6): 997-1002.

[7] WEN Xiao-jun, LIU Yun, SUN Yu. Quantum multi signature protocol based on teleportation[J]. Zeitschrift Fur Naturforschung A, 2007, 62(3/4): 147-151.

[8] ZHOU Nan-run, LIU Yun, ZENG Gui-hua, *et al*. Novel qubit blockencryption algorithm with hybrid keys[J]. Physica A, 2007, 375(2): 693-702.

[9] CHIRIBELLA G, D'ARIANO G M, PERINOTTI P. Theoretical framework for quantum networks[J]. Physical Review A, 2009, 80(2): 022339-022358.