基于 Bell 态纠缠交换的量子盲签名方案

郑 涛 张仕斌* 昌 燕 李雪杨
(成都信息工程大学 四川 成都 610225)

摘 要 基于量子纠缠交换理论,提出一种基于 Bell 态纠缠交换的量子盲签名方案。消息拥有者 Alice 将待签名消息发送给盲签名者 Charlie,Charlie 根据双方共享的量子密钥对消息进行盲化签名,加密后发送给消息验证者 Bob。Bob 收到盲化签名后,根据他与 Charlie 共享的量子密钥对签名进行验证。利用量子纠缠特性,实现了消息对签名者 Charlie 的盲化性。基于量子密钥分发和一次一密技术,保证了签名过程的绝对安全性。

关键词 量子纠缠 盲签名 Bell 态

中图分类号 TP309 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.03.052

QUANTUM BLIND SIGNATURE SCHEME BASED ON BELL STATE ENTANGLEMENT SWAPPING

Zheng Tao Zhang Shibin* Chang Yan Li Xueyang
(*Chengdu University of Information Technology*, *Chengdu 610225*, *Sichuan*, *China*)

Abstract Based on the theory of quantum entanglement swapping, this paper proposes a quantum blind signature scheme based on Bell state entanglement swapping. Message owner Alice sent the message to be signed to the blind signer Charlie, who blindly signed the message according to the quantum key shared by both parties, and he sent it to the message verifier Bob after encryption. After receiving the blind signature, Bob verified the signature according to the quantum key that he shared with Charlie. By using quantum entanglement, blindness of the message to signer Charlie was realized. Based on quantum key distribution and one-time one-key technology, the absolute security of the signature process is guaranteed.

Keywords Quantum entanglement Blind signature Bell state

0 引 言

1984 年 Bennett 和 Brassard 提出了第一个量子密码协议,即 BB84 协议[1]。随后科研工作者们提出了大量的量子密码协议与量子通信协议,包括量子密钥分发协议(QKD)[2-4]、量子直接安全通信协议(QSDC)[5-7]、量子秘密共享协议(QSS)[8-9]、量子隐私查询协议(QPQ)[10-15]等。

电子签名的概念由 Diffie 和 Hellman 在 1976 年第一次提出[11],1983 年 Chaum 等基于电子签名提出了盲签名的概念。盲签名协议的基本要求有:(1)不可伪造性,除签名人之外没有人可以伪造签名。(2)不可否认性,消息拥有者和签名人都不能否认自己对消息的操作。(3)盲性,签名者不能将自己的签名与消息对应起来。盲签名方案在现实生活中有着广泛的应用,比如匿名选举、电子现金交易等。

随着量子技术的不断发展,量子计算机的出现将会使基于数学计算复杂性的签名方案变得不再安全。研究人员在过去的十多年内开始研究基于量子信息的签名协议。2001 年 Gottsman 等[16]提出了基于量子单向函数的签名方案。曾贵华等[17]于同年提出了基于

收稿日期:2019-03-27。国家自然科学基金项目(61572086,61402058);国家重点研发计划项目(2017YFB0802302);四川省重点研发计划项目(2018TJPT0012);四川省高校科研创新团队项目(17TD0009);四川省学术和技术带头人培养支持经费项目(2016120080102643);四川省应用基础项目(2017JY0168);四川省科技支撑计划项目(2016FZ0112,2018GZ0204)。**郑涛**,硕士生,主研领域:量子安全通信。**张仕斌**,教授。**昌燕**,教授。**李雪杨**,硕士生。

GHZ 态的量子仲裁签名方案。这两个方案都要求一个可信的第三方来完成认证。2009 年温晓军等[18]提出了基于量子密钥的弱盲签名协议,2010 年他们又提出了基于量子秘密共享的强盲签名协议[19]。2011 年陈永志等[20]提出了基于可控形态的代理弱盲签名协议。随后出现了一系列基于量子密钥的盲签名协议[21-27]。

本文提出了一种基于 Bell 态纠缠交换的盲签名协议,消息拥有者与签名者使用量子密钥分发技术共享密钥对消息进行加密,协议使用一次一密技术保证整个签名过程的绝对安全性。

1　准备知识

1.1　纠缠交换

四种 Bell 态粒子描述如下:

$$|\phi^{\pm}\rangle_{12}=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle)_{12}$$

$$|\psi^{\pm}\rangle_{12}=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle)_{12}$$

假设 Alice 拥有 Bell 态粒子 $|\phi^{+}\rangle_{12}$,Bob 拥有 $|\phi^{+}\rangle_{34}$,经过 Bell 纠缠交换,量子系统变化为:

$$|\phi^{+}\rangle_{12}\otimes|\phi^{+}\rangle_{34}=\frac{1}{2}\left(\begin{array}{l}|\phi^{+}\rangle_{13}\otimes|\phi^{+}\rangle_{24}+|\phi^{-}\rangle_{13}\otimes\\|\phi^{-}\rangle_{24}+|\psi^{+}\rangle_{13}\otimes|\psi^{+}\rangle_{24}+\\|\psi^{-}\rangle_{13}\otimes|\psi^{-}\rangle_{24}\end{array}\right)\tag{1}$$

当对粒子 1 和粒子 3 执行 Bell 基测量时,粒子 2 和粒子 4 塌缩到对应的纠缠状态。比如 Alice 对粒子 1 和粒子 3 的 Bell 基测量结果为 $|\psi^{+}\rangle_{13}$,则 Bob 对粒子 2 和粒子 4 的测量结果为 $|\psi^{+}\rangle_{24}$。

1.2　量子逻辑操作

四种常见的量子逻辑操作(泡利操作符)表示为:

$$\sigma_{00}=I=|0\rangle\langle 0|+|1\rangle\langle 1|$$

$$\sigma_{01}=\sigma_x=|0\rangle\langle 1|+|1\rangle\langle 0|$$

$$\sigma_{10}=i\sigma_y=|0\rangle\langle 1|-|1\rangle\langle 0|$$

$$\sigma_{11}=\sigma_z=|0\rangle\langle 0|-|1\rangle\langle 1|$$

以 Bell 态 $|\phi^{+}\rangle_{AB}$为例,经过泡利操作符作用后,量子态变化情况如表 1 所示。

表 1　Puali 操作与 Bell 态粒子的测量结果

	σ_{00}	σ_{01}	σ_{10}	σ_{11}
σ_{00}	$\|\phi^{+}\rangle_{AB}$	$\|\psi^{+}\rangle_{AB}$	$\|\psi^{-}\rangle_{AB}$	$\|\phi^{-}\rangle_{AB}$
σ_{01}	$\|\psi^{+}\rangle_{AB}$	$\|\phi^{+}\rangle_{AB}$	$\|\phi^{-}\rangle_{AB}$	$\|\psi^{-}\rangle_{AB}$
σ_{10}	$\|\psi^{-}\rangle_{AB}$	$\|\phi^{-}\rangle_{AB}$	$\|\phi^{+}\rangle_{AB}$	$\|\psi^{+}\rangle_{AB}$
σ_{11}	$\|\phi^{-}\rangle_{AB}$	$\|\psi^{-}\rangle_{AB}$	$\|\psi^{+}\rangle_{AB}$	$\|\phi^{+}\rangle_{AB}$

2　量子盲签名方案

2.1　初始化阶段

(1) 消息变换:Alice 将待签名消息 m 转换成二进制序列 $M=T_2(m_1,m_2,\cdots,m_n)\in\{0,1\}^n$。$T_2$代表一个二进制转换函数。

(2) 密钥共享:假定 Alice 是消息拥有者,Bob 是消息确认者,Charlie 是盲签名者。通过量子密钥分发技术(Quantum Key Distribution,QKD),Alice 与 Bob 秘密共享 key_{AB},Alice 与 Charlie 秘密共享 key_{AC},Bob 与 Charlie 秘密共享 key_{BC}。QKD 的物理安全特性保证密钥分发过程的绝对安全性。

(3) 粒子制备与分发:Charlie 制备两串长度为 n 的 Bell 态粒子序列,n 代表消息的长度。为方便描述,假定两串 Bell 态处于 $|\phi^{+}\rangle_{12}$和 $|\phi^{+}\rangle_{34}$(其余状态的签名过程类似),Charlie 按粒子下标将其分成序列 $P=\{S_1,S_2,S_3,S_4\}$,其中 S_i代表两串 Bell 态中所有下标为 i 的粒子组成的序列。Charlie 将 S_1S_3发送给 Alice,将 S_2发送给 Bob,自己保留 S_4。

2.2　签名阶段

(1) 消息编码与发送:Alice 根据二进制消息 M 的值,选择相应的泡利操作对粒子序列 S_1S_3进行量子门变换,完成消息绑定。消息转变规则如表 2 所示。其中:$M_i=0$,执行泡利 I 操作;$M_i=1$,执行泡利 $i\sigma_y$操作。完成转换后,粒子序列变为 $S_1'S_3'$。Alice 使用 Bell 基测量 $S_1'S_3'$ 得到 Q_1Q_3,此时 S_2S_4塌缩到对应的状态然后使用一个与 *Bob* 秘密约定的转换函数 H 将 $S_1'S_3'$ 的测量结果转换成 $R_1R_3=H(Q_1Q_3)$;Alice 使用 key_{AB}加密 R_1R_3,得到 $E_{key_{AB}}(R_1R_3)$,并将 $E_{key_{AB}}(R_1R_3)$发送给 Charlie;Alice 使用 key_{AB}加密二进制消息 M,得到 $X=E_{key_{AB}}(M)$并发送给 Bob。

表 2　二进制消息 M 经量子门转换后的变换情况

M_i	泡利操作	S_1S_3	$S_1'S_3'$
0	I	$\|\phi^{+}\rangle_{13}$	$\|\phi^{+}\rangle_{13}$
		$\|\phi^{-}\rangle_{13}$	$\|\phi^{-}\rangle_{13}$
		$\|\psi^{+}\rangle_{13}$	$\|\psi^{+}\rangle_{13}$
		$\|\psi^{-}\rangle_{13}$	$\|\psi^{-}\rangle_{13}$
1	$i\sigma_y$	$\|\phi^{+}\rangle_{13}$	$\|\psi^{-}\rangle_{13}$
		$\|\phi^{-}\rangle_{13}$	$-\|\psi^{+}\rangle_{13}$
		$\|\psi^{+}\rangle_{13}$	$\|\phi^{-}\rangle_{13}$
		$\|\psi^{-}\rangle_{13}$	$-\|\phi^{+}\rangle_{13}$

(2) 盲签名:Charlie 收到 $E_{key_{AB}}(R_1R_3)$ 后,使用 Z 基($|0\rangle$,$|1\rangle$)或 X 基($|+\rangle$,$|-\rangle$)对自己保留的 S_4 进行测量,得到测量结果 R_4。Charlie 使用 key_{BC} 加密 R_4 和 $E_{key_{AB}}(R_1R_3)$,得到 $E_{key_{BC}}(R_4, E_{key_{AB}}(R_1R_3))$。Charlie 将 $E_{key_{BC}}(R_4, E_{key_{AB}}(R_1R_3))$ 发送给 Bob。

2.3 验证签名阶段

(1) Bob 接收了 Charlie 发送的加密序列后 $E_{key_{BC}}(R_4, E_{key_{AB}}(R_1R_3))$,使用 key_{BC} 解密后获得 R_4 和 $E_{key_{AB}}(R_1R_3)$,再使用 key_{AB} 解密 $E_{key_{AB}}(R_1R_3)$ 获得 R_1R_3;根据 R_4,Bob 选择相同的测量基对 S_2 进行测量,得到 R_2。此时 Alice 告知 Bob 她对消息 M 的绑定规则。

(2) Bob 根据接收的 R_1R_3,通过与 Alice 秘密约定的转换函数 H 将 R_1R_3 转换成 $S'_1S'_3 = H(R_1R_3)$;根据接收的 R_4,结合自己测量得到的 R_2,通过量子纠缠交换关系(式(1))可以得出 S_2 和 S_4 对应的 Bell 粒子状态。如表 3 所示,Bob 可以推测出 Alice 对粒子序列 S_1S_3 执行的泡利操作序列,进而推出粒子序列 $S_1^dS_3^d$。由表 2 的消息绑定规则可以得到 M^d,Bob 使用 key_{AB} 解密 $X = E_{key_{AB}}(M)$ 得到 M;Bob 比较 $M^d = M$ 以及 $S_1^dS_3^d = S'_1S'_3$ 是否均成立,若两个等式都成立则接受 Charlie 的签名,否则拒绝签名。

表 3 验证规则

M_i	泡利操作	S_1S_3	测量基	S_2S_4
0	I	$\|\phi^+\rangle_{13}$	X	$\|\phi^+\rangle_{24}$
		$\|\phi^-\rangle_{13}$	Z	$\|\phi^-\rangle_{24}$
		$\|\psi^+\rangle_{13}$	Z	$\|\psi^+\rangle_{24}$
		$\|\psi^-\rangle_{13}$	X	$\|\psi^-\rangle_{34}$
1	$i\sigma_y$	$\|\psi^-\rangle_{13}$	X	$\|\phi^+\rangle_{24}$
		$-\|\psi^+\rangle_{13}$	Z	$\|\phi^-\rangle_{24}$
		$\|\phi^-\rangle_{13}$	Z	$\|\psi^+\rangle_{24}$
		$-\|\phi^+\rangle_{13}$	X	$\|\psi^-\rangle_{34}$

3 方案分析

3.1 无条件安全性

在本协议中,Alice 与 Bob、Charlie 三方分别秘密共享的密钥都是通过量子密钥分配技术(quantum key distribution,QKD)在量子信道中完成分发的。量子密钥分配技术结合一次一密(one-time pad,OTP)在理论和实践中都已经被证明是绝对安全可靠的,因此密钥 key_{AB} 和 key_{BC} 以及 key_{AC} 均是绝对安全的。

如果攻击者 Eve 采用截获重发攻击(一种强有力的攻击方式),量子的不可克隆性保证了 Bell 态粒子是不可被复制的,Eve 对截获的粒子进行测量等操作势必会破坏 Bell 态粒子的纠缠关系,Alice 签名信息相应会产生扰动,Charlie 将拒绝签名;同理,三方均可以通过分析粒子纠缠关系以及检测量子信道等方式来检测是否存在窃听者。若发现窃听者存在,协议终止。需要注意的是,由于 Alice 通过泡利操作将消息编码在 S_1S_3 中,假设 Eve 侥幸避开检测,也得不到任何有用的信息。

3.2 不可伪造性

假设 Alice 或 Eve 是不诚实的用户,她们想伪造签名者 Charlie 来对消息进行签名,达到欺骗的目的。通过分析协议可以得知:key_{BC} 是 Charlie 和 Bob 通过 QKD 和 OTP 进行安全保障的,Alice 或 Eve 在不知道 key_{BC} 的情况下是不可能得到加密序列 $E_{key_{BC}}(R_4, E_{key_{AB}}(R_1R_3))$;与此同时,Charlie 将自己对 S_4 的测量结果 R_4 也放在盲签名序列中,Alice 或 Eve 无法得知 R_4 的正确信息,因此本协议产生的盲签名是不可伪造的。

3.3 不可抵赖性

根据协议的描述,Charlie 是无法否认自己的盲签名信息:Bob 接收的加密序列使用的密钥必须为 Bob 与 Charlie 秘密共享的 key_{BC};同理,Charlie 收到的加密序列 $E_{key_{AB}}(R_1R_3)$ 必须由密钥 key_{AB} 加密,当 Bob 使用 key_{BC} 解密了 $E_{key_{BC}}(R_4, E_{key_{AB}}(R_1R_3))$ 后,只能使用 key_{AB} 才能解密出正确的 R_1R_3,因此 Alice 也无法否认自己对消息的编码操作。

3.4 消息盲性

在本协议中,Charlie 在执行签名的过程中,所有消息内容都是 Alice 通过 key_{AB} 加密的 $E_{key_{AB}}(R_1R_3)$,Charlie 无法在签名时获取任何和消息相关的内容。签名完成后,Alice 与 Bob 的信息交换均不涉及原始的消息,而是通过对量子序列的操作。即 Charlie 无法将自己的签名与 Alice 的消息对应起来,达到了盲签名效果。

3.5 效率分析

量子签名协议的效率可以用如下公式计算:

$$\eta_e = \frac{\eta_c}{\eta_t}$$

式中:η_c 代表待签名消息的比特数目,η_t 代表协议用到的粒子总数。因此本协议的粒子效率为:$\eta_e = \frac{2n}{7n+0} \times 100\% = 28.6\%$,对比现有的协议[25-27],本协议在效率上有一定的提升。粒子的效率比较如表 4 所示,其中

文献[25 – 27]简记为协议 1、协议 2、协议 3。

表 4　效率分析

协议	协议 1	协议 2	协议 3	本协议
粒子效率	25%	22.2%	18.2%	28.6%

4　结　语

本文基于 Bell 态纠缠变换关系,提出了一个量子盲签名协议,消息拥有者对粒子序列执行泡利操作完成经典消息向量子消息的转变。三个参与方通过分别共享的量子密钥保证了协议的绝对安全性。通过方案分析可知本协议满足盲签名定义,通过效率分析可知完成 n 比特消息的盲签名,本协议的粒子效率为 28.6%。由于现实通信环境的噪音等干扰因素,实际粒子效率可能偏低。

参 考 文 献

[1] Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing[C]//Proc of IEEE International Conference on Computers Systems and Signal Processing. 1984: 175 – 179.

[2] Bennett C H. Quantum cryptography using any two nonorthogonal states[J]. Physical Review Letters, 1992, 68(68): 3121 – 3124.

[3] Wang C, Wang S, Yin Z Q, et al. Experimental measurement-device-independent quantum key distribution with uncharacterized encoding[J]. Optics Letters, 2016, 41(23): 5596 – 5599.

[4] Curty M, Xu F H, Cui W, et al. Finite-key analysis for measurement-device-independent quantum key distribution [J]. Nature Communications, 2014, 5(4):643 – 648.

[5] Patwardhan S, Moulick S R, Panigrahi P K. Efficient controlled quantum secure direct communication protocols[J]. International Journal of Theoretical Physics, 2016, 55(7): 3280 – 3288.

[6] Chang Y, Xu C X, Zhang S B, et al. Quantum secure direct communication and authentication protocol with single photons[J]. Chinese Science Bulletin, 2013, 58(36): 4571 – 4576.

[7] Cai Q Y, Li B W. Deterministic secure communication without using entanglement[J]. Chinese Physics Letters, 2004, 21(4):601 – 603.

[8] Qin H W, Dai Y W. Verifiable(t, n) threshold quantum secret sharing using d-dimensional Bell state[J]. Information Processing Letters, 2016, 116(5):351 – 355.

[9] Mishra S, Shukla C, Pathak A, et al. An integrated hierarchical dynamic quantum secret sharing protocol[J]. International Journal of Theoretical Physics, 2015, 54(9):1 – 12.

[10] Gertner Y, Ishai Y, Kushilevitz E, et al. Protecting data privacy in private information retrieval schemes[J]. Journal of Computer and System Sciences, 2000, 60(3):592 – 629.

[11] Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6), 644 – 654.

[12] Olejnik L. Secure quantum private information retrieval using phase-encoded queries[J]. Physical Review A, 2011, 84(2): 3242 – 3244.

[13] Jakobi M, Simon C, Gisin N, et al. Practical private database queries based on a quantum-key-distribution protocol [J]. Physical Review A, 2011, 83(2):022301.

[14] Gao F, Liu B, Wen Q Y, et al. Flexible quantum private queries based on quantum key distribution[J]. Optics Express, 2012, 20(16):17411.

[15] Liu B, Gao F, Huang W, et al. QKD-based quantum private query without a failure probability[J]. Science China: Physics, Mechanics and Astronomy, 2015, 58(10):100301.

[16] Gottesman D, Chuang I. Quantum digital signatures[EB]. arXiv:quant-ph/0105032, 2001.

[17] 曾贵华, 马文平, 王新梅, 等. 基于量子密码的签名方案[J]. 电子学报. 2001, 29(8): 1098 – 1100.

[18] Wen X J, Niu X M, Ji L P, et al. A weak blind signature scheme based on quantum cryptography[J]. Optics Communications, 2009, 282: 666 – 669.

[19] 温晓军,田原,牛夏牧. 一种基于秘密共享的量子强盲签名协议[J]. 电子学报, 2010, 38(3): 720 – 724.

[20] 陈永志, 刘云, 温晓军. 一个量子代理弱盲签名方案[J]. 量子电子学报, 2011, 28(3): 341 – 349.

[21] Guo Y, Feng Y, Huang D, et al. Arbitrated quantum signature scheme with continuous-variable coherent states[J]. International Journal of Theoretical Physics, 2016, 55(4): 2290 – 2302.

[22] Tian J H. A Quantum multi-proxy blind signature scheme based on genuine four-qubit entangled state[J]. International Journal of Theoretical Physics, 2016, 55(2):809 – 816.

[23] Yang Y G, Lei H, Liu Z C, et al. Arbitrated quantum signature scheme based on cluster states[J]. Quantum Information Processing, 2016, 15(6):2487 – 2497.

[24] Pan J, Zhou L, Gu S P, et al. Efficient entanglement concentration for concatenated Greenberger-Horne-Zeilinger state with the cross-Kerr nonlinearity[J]. Quantum Information Processing, 2016, 15(4):1669 – 1687.

[25] Zhang J Z, Yang Y Y, Xie S C. A third-party E-payment protocol based on quantum group blind signature[J]. International Journal of Theoretical Physics, 2017, 56(9):2981 – 2989.

(下转第 333 页)

量;P 表示伪随机数函数的计算量;M 表示模运算的计算量;C 表示交叉运算的计算量;XOR 表示异或运算的计算量;Sac 表示自组合交叉位运算的计算量。所有的通信消息长度均用 l 表示。

上述运算可以分为两种,一种是轻量级的计算量,另一种是超轻量级的计算量。H、PR、PUF、P、M 这几种运算均属于轻量级的计算;C、XOR、Sac 这几种运算均属于超轻量级的计算。根据不同量级的运算定义,轻量级的计算量一般是超轻量级的计算量的若干倍。由表 3 可知,除本文协议之外,其他协议均存在轻量级的运算,因此在标签一端的计算量方面,本文协议具有一定的优势。从标签的存储空间角度出发,可以看出本文协议与其他文献中所提出的协议在数据的存储量方面是相当的。基于性能分析和安全性分析,本文协议在标签一端的计算量方面有一定的改进和提升,同时也能够弥补其他协议存在的安全缺陷问题。

6 结　语

传统的 RFID 系统在广泛运用的同时,逐渐面临新的困境。移动式的 RFID 系统的出现能够很好地弥补传统 RFID 系统的不足,但其无法提供通信信息的安全。为了确保通信消息的安全,本文设计了适用于移动式的 RFID 系统双向认证协议。在 Wang 等所提的协议基础上,给出改进的协议。改进的协议必须在通信实体之间完成双向认证之后,才会进行后续的操作,从而可以避免攻击者的重放攻击及假冒攻击;同时为能够抵抗攻击者其他类型的攻击,通信信息均加密后再传输,且加密过程中均混入随机数,使得攻击者无法通过当前窃听的信息推导出上一轮或下次的通信消息。对协议进行安全性分析,表明协议能够满足移动式的 RFID 系统的安全需求;对协议进行性能分析,表明协议在计算量方面能够适用于当前的移动式 RFID 系统中。下一步研究方向:将加载有该协议的移动式 RFID 系统原型实现出来,研究一个完整通信所需时间及计算量等具体参数。

参 考 文 献

[1] Xie R, Jian B Y, Liu D W. An improved ownership transfer for RFID protocol[J]. International Journal of Network Security, 2018, 20(1): 149 - 156.

[2] 刘道微,凌捷. 一种改进的满足后向隐私的 RFID 认证协议[J]. 计算机科学,2016,43(8):128 - 130.

[3] Huang Z, Xu R, Chu C, et al. A novel cross layer anti-collision algorithm for slotted ALOHA-based UHF RFID systems [J]. IEEE Access, 2019, 7: 36207 - 36217.

[4] Sidorov M, Ong M T, Sridharan R V, et al. Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains[J]. IEEE Access,2019, 7: 7273 - 7285.

[5] 刘鹏. 一种 RFID 系统多标签共存证明协议设计[J]. 兵器装备工程学报,2018,39(2):124 - 126.

[6] Xu H, Shen W W, Li P, et al. Novel implementation of defence strategy of relay attack based on cloud in RFID systems [J]. IJICS,2019, 11(2): 120 - 144.

[7] Xie R, Ling J, Liu D W. Wireless key generation algorithm for RFID system based on bit operation[J]. International Journal of Network Security, 2018, 20(5): 938 - 949.

[8] Zhang Y L, Chen S G, Zhou Y, et al. Monitoring bodily oscillation with RFID tags[J]. IEEE Internet of Things Journal,2019, 6(2): 3840 - 3854.

[9] 王国伟,贾宗璞,彭维平. 基于动态共享密钥的移动 RFID 双向认证协议[J]. 电子学报,2017,45(3):612 - 618.

[10] 占善华. 基于交叉位运算的移动 RFID 双向认证协议[J]. 计算机工程与应用,2019,55(7):120 - 126.

[11] Kaul S D, Awasthi A K. Privacy model for threshold RFID system based on PUF[J]. Wireless Personal Communications, 2017, 95(3): 2803 - 2828.

[12] Sundaresan S, Doss R, Piramuthu S, et al. A secure search protocol for low cost passive RFID tags[J]. Computer Networks, 2017, 122: 70 - 82.

[13] Fan K, Jiang W, Li H, et al. Lightweight RFID protocol for medical privacy protection in IoT[J]. IEEE Transactions on Industrial Informatics, 2018, 14(4): 1656 - 1665.

[14] 汪杰,汪学明. 改进的轻量级移动 RFID 双向认证协议[J]. 计算机工程与设计,2018,39(4):912 - 917.

[15] Fan K, Zhu S S, Zhang K, et al. A lightweight authentication scheme for cloud based RFID healthcare systems[J]. IEEE Network,2019, 33(2): 44 - 49.

[16] Ibrahim A, Dalkiliç G. Review of different classes of RFID authentication protocols [J]. Wireless Networks, 2019, 25(3):961 - 974.

[17] Bai Z, He Y G. Recognition of the anti-collision algorithm for RFID systems based on tag grouping[J]. IJICT,2019, 14(1): 81 - 88.

(上接第 313 页)

[26] Fan L. A blind signature protocol with exchangeable signature sequence[J]. International Journal of Theoretical Physics, 2018, 57(12):3850 - 3858.

[27] Liang X Q, Wu Y L, Zhang Y H, et al. Quantum multi-proxy blind signature scheme based on four-qubit cluster states[J]. International Journal of Theoretical Physics,2019, 58(1):31 - 39.