无条件安全的量子茫然传送

杨 威, 黄刘生, 罗永龙, 陈国良
(1. 中国科学技术大学计算机科学与技术系, 安徽合肥 230027; 2. 安徽省计算与通讯软件重点实验室, 安徽合肥 230027;
3. 中国科学技术大学苏州研究院, 江苏苏州 215123)

摘 要: 茫然传送作为安全多方计算的基础协议具有重要的理论研究和实用价值. 目前已有的经典环境中的各茫然传送协议大都基于公钥密码学或一些附加的计算困难性假设, 而这些基础在量子计算机制下将变得相当脆弱. 本文根据量子贝尔态的特性, 提出了一种新的量子茫然传送协议, 对其正确性与安全性进行了分析与证明. 该协议可同时抵抗通信信道中噪声和可能存在的窃听, 在安全性、健壮性、窃听检测等方面均优于经典计算环境下的各种茫然传送协议.

关键词: 茫然传送; 保密增强; 贝尔态; 无条件安全
中图分类号: TN393 文献标识码: A 文章编号: 0372-2112 (2007) 08-1543-05

Unconditionally Secure Quantum Oblivious Transfer

YANG Wei, HUANG Liu-sheng, LUO Yong-long, CHEN Guo-liang
(1. *Department of Computer Science and Technology, University of Science and Technology of China, Hefei, Anhui 230027, China;*
2. *Anhui Province Key Laboratory of Software in Computing and Communication, Hefei, Anhui 230027, China;*
3. *Suzhou Institute for Advanced study, USTC, Suzhou, Jiangsu 215123, China*)

Abstract: As a basic protocol of Secure Multi-party Computation, Oblivious Transfer (OT) is of significant research and application value. Most of previous oblivious transfer protocols in classical environment rely either on public-key cryptography or on additional computational assumptions which will be very vulnerable under quantum mechanics. Based on the characteristics of Bell States, a new quantum oblivious transfer protocol is proposed in this paper. The correctness and security of the protocol are analyzed and proved. The protocol is secure in the presence of noise on the channel and a potential eavesdropper. Comparing with oblivious transfer protocols in classical computational environment, the protocol in this paper is superior in security, soundness and wire-tapping detecting.

Key words: oblivious transfer; privacy amplification; bell states; unconditionally secure

1 引言

简单地说, 茫然传送(Oblivious Transfer, OT)指的是这样一种密码学模型: 接收者可以从发送者的秘密消息集合中获取自己想要的消息(但不能获取其他的消息), 而发送者不知道接收者选择的是哪条消息. 不失一般性, 我们可以假定消息内容为单个比特. 茫然传送是现代密码学中重要的基础协议, 目前广泛用于构建零知识证明、可验证秘密分享、安全多方计算等协议, 同时和比特承诺一起构成双方安全计算的基础, 是信息安全领域研究的热点.

茫然传送的概念最早由 Rabin 在文献[1]中提出, 随后该概念被 Even 等人在文献[2]中发展为二中选一的 OT, 记为$\binom{2}{1}$-OT. 文献[3]使用其自定义的一种 pr-OT 证明了 Rabin 的原始 OT 和$\binom{2}{1}$-OT 具有等价性——二者可以互相归约. $\binom{2}{1}$-OT 是目前最为广泛接受和使用的 OT 模型, 其一般性的定义如下:

定义 **1** $\binom{2}{1}$-OT 模型: Alice 拥有两个比特 b_0 和 b_1, Bob 可以选择了解其中之一 b_c ($c \in \{0, 1\}$). 协议的结果要求:

(1) Bob 只能正确获得 b_c 而无法了解 b_{1-c} 的信息;

(2) Alice 不知道 Bob 的选择 c.

收稿日期: 2006-02-24; 修回日期: 2007-03-08
基金项目: 国家自然基金(No. 60573171); 教育部博士点基金(No. 20060358014); 江苏省自然科学基金(No. BK2007060)

后来发展的很多种 OT 的新模型, 如$\binom{2}{1}$-OT^k、AN-DOS(All-or-nothing disclosure of secrets)、GOT(Generalized OT)等一般都可以归约为$\binom{2}{1}$-OT[2,4,5]. 文献[6]提出了 UOT(Universal OT), 并证明了$\binom{2}{1}$-OT 可以归约为更广义的 UOT.

传统的经典计算环境中的茫然传送协议存在不少问题, 例如文献[1, 2]等基于大数分解、离散对数等 NP 难解问题, 文献[7~10]则为了协议的安全性做了附加的限制性假设. 这些方案要么在强大的量子计算机面前不堪一击, 要么使用了辅助的第三方来完成部分计算任务, 而实际应用中很难找到可信的甚至是茫然的第三方.

本文给出一个在量子计算环境下的 OT 协议, 并证明其正确性与安全性. 本文构建的量子 OT 协议不对协议参与方的计算能力做任何限制性假设, 而且没有使用可信或半可信第三方, 同时量子信道中的任何窃听都可以被有效地检测出来, 在安全性、健壮性、抗窃听性等方面均优于经典环境中的各类 OT 方案.

2 基于 EPR 纠缠的量子茫然传送协议

在量子通信过程中, 最理想的情况是信道无噪声且不存在第三方的窃听者. 然而实际上噪声总是无可避免的客观存在, 窃听者也有其存在的可能. 早期的 QOT 协议[11,12]未考虑噪声与容错的情况, 因而是不切实际的. 文献[15]的 QOT 协议考虑了信道存在的噪声情况, 但却没有讨论窃听者 Eve 存在的条件下, 协议是否仍然有效的问题. 本文的协议则兼顾地考虑了 Eve 与噪声都有可能存在的情况.

有别于文献[15]的单光子通信模型, 本文的协议采用处于四个贝尔态之一的光子对来完成协议初始阶段的通信任务. 下面先给出理想情况下(无噪无窃听)的协议模型:

Protocol1 QOT(b_0, b_1)

Step1 Alice 制备 $2s+2N$ 对处于式(3)~(6)中任一式(例如$|\Psi^-\rangle$)的纠缠光子对, 自己保留每一对的光子 1, 并将光子 2 发送给 Bob. 其中, s 是 Alice 选定的安全参数.

Step2 Alice 对于每一纠缠对中的光子 1, 均匀随机地选择+基或×基进行测量, 并记录测量结果.

Step3 Bob 对于接收到的每一对中的光子 2, 均匀随机地选择+基或×基进行测量, 并记录测量结果.

Step4 对于 $2s+2N$ 个光子, Alice 均要求 Bob 对其测量结果作出承诺. 然后 Alice 任意选择其中的 $2s$ 个, 要求 Bob 出示他选择的测量基与测量结果. Bob 照做后, Alice 验证同 Bob 选择的基相同的每一个光子, 其测量结果是否与其承诺一致. 如果验证无误, Alice 通知 Bob, 他通过了验证, 转 Step 5; 否则 Alice 认为 Bob 作弊, 协议终止.

Step5 如果 Bob 通过验证, 他要求 Alice 公开她对剩下 $2N$ 个光子选择的测量基. 收到结果后, 他把这 $2N$ 个光子分成两组: 一组是跟 Alice 选择的基相同, 记为 R_d($d\in\{0,1\}$, 如果本组中的第一个元素地址(编号)是 $2N$ 个光子中最低的, 则 d 取 0, 反之取 1); 另一组跟 Alice 选择的基相反, 记为 R_{1-d}. 由双方选择测量基时的均匀随机特性知, 两组所包含的光子数基本相同. 如果稍微不等, 则将光子数目略多的那一组多于 N 的高地址部分附在另外一组的后面, 这样就保证 $|R_0|=|R_1|=N$. Bob 随后告诉 Alice R_0 和 R_1 中所有光子的地址. 同时, Bob 将他的选择(即 b_c 中的 c)与 d 异或的结果 e(即 $e=c\oplus d$)发送给 Alice.

Step6 Alice 对于 R_0 和 R_1 均取其前 n 个地址(n 只要保证略小于 Bob 测量的两组中势稍小的那一组的基数即可), 对应这 $2n$ 个光子的测量结果记录产生了两个 bit 串 r_0 和 r_1. 然后 Alice 计算 $q_0=\bigoplus_{i=1}^{n} r_0$, $q_1=\bigoplus_{i=1}^{n} r_1$, $f_0=b_0\oplus q_e$, $f_1=b_1\oplus q_{1-e}$, 并将 f_0、f_1 和 n 发送给 Bob.

Step7 Bob 计算 $q_d=\bigoplus_{i=1}^{n} r_d$, $b_c=f_c\oplus q_d$ 得到自己想要的比特.

上述的协议是针对理想情况的, 实际的通信信道总是需要考虑噪声与窃听, 分别讨论如下:

对于窃听者 Eve 的检测其实很简单, 只要 Alice 在协议中多发送给 Bob t 个光子, 然后与 Bob 约定对这 t 个光子做相同的测量后, 再公开比较测量结果, 如果测量结果相关联, 说明无窃听; 若结果不关联(超过一定概率的不关联), 则可以判定信道上存在窃听. 由量子不可克隆定理可以保证结论的正确性.

在实际实验中使用的信道都是不可避免的受到环境噪声的影响的, 信道噪声的存在使得传送的最大纠缠态退化成混合态, 并且纠缠度也减少了. 在这种情况下, 我们调用文献[13]中提出的保密增强方案 QPA 作为一个子协议来解决纠缠度减少的问题(关于保密增强的进一步知识, 请参考文献[14]). 该方案的另外一个好处就是, 即使窃听存在, QPA 仍然有效, 使得茫然传送协议可以继续进行, 而不是像一般情况那样, 检测到窃听后就终止协议.

3 协议的分析与证明

由通信过程以及量子机制可见, 如果双方均忠实

地执行协议,则可以得到$\binom{2}{1}$-OT 的结果. 事实上,如果 Alice 主动作弊,例如发送给 Bob 的两个比特或比特串都是垃圾(junk),则目前没有任意一种 OT 协议可以阻止 Alice 这样做,然而我们却不需要为此担心,因为这个事件是平凡的,$\binom{2}{1}$-OT 模型的本身就蕴涵了这层意思,即 Alice"需要"向 Bob 茫然传送她的两个比特之一. 更多的讨论,见文献[16].所以,本文的安全性分析主要是针对 Alice 企图得知 Bob 选定的 c 与 Bob 为获得更多的信息(如 b_{1-c})而可能采取的各种手段,以及协议抵抗这些攻击的能力.

3.1　Alice 的攻击分析

Alice 的目标首先是成功向 Bob 传送她的两个比特之一,除此之外,"贪心"的 Alice 可能想知道 Bob 到底选的是哪个比特,对于此,我们有:

定理 1　在 QOT(b_0, b_1)协议之后,Alice 无法得知 Bob 的选择 c.

证明　对于 Alice,她只有在 Step 5 中尽可能地了解 Bob 选择的 c. 但是注意到 Bob 从来没有直接提供 c 的信息,事实上,考虑到 d 只有 Bob 知道,c 与 d 异或的结果 e 对 Alice 来说也是完全随机的,她无法从 e 中得知 c 的任何信息. 这样,从信息论的角度来说,尽管可以认为 Alice 的计算能力是无限的(相对于经典计算环境),她也没有作弊的可能.

3.2　Bob 的攻击分析

较之 Alice,Bob 的可能欺骗方式要多样化一点,他有可能在 Step3 与 Step5 中采取多种攻击方式来获取的 b_{1-c} 信息.

3.2.1　光子存储攻击

对于 Bob,假设他在 Step 3 使用光子存储攻击,即先不测量 Alice 传送的光子,而是保存至 Alice 公开她对 2N 个光子的测量基以后再进行测量. 那么,这种攻击方式的成功率如何呢?

定理 2　即使使用光子存储攻击,Bob 在 QOT(b_0, b_1)中成功的概率也是可以忽略的.

证明　如果在 Step 4 中 Alice 不要求 Bob 作出 bit 承诺的话,那么 Bob 的确可以同时获得 b_0 和 b_1. 而引入承诺后,Bob 作弊成功的机会仅为 $1/2^s$ ——对于 $2s$ 个光子的承诺,Bob 伪造的测量结果应该保证有 s 个跟 Alice 的测量基相同,另外 s 个相异(他只要均匀选择 s 个+ 基和 s 个 × 基即可).对于相异的基,Alice 可以放过,而对于相同的基,Alice 要验证结果是否一致. 对于每个基伪造的测量结果,Bob 只能在 0 和 1 之间随机选一个,这样他每个相同基光子作弊成功的概率为 1/2,对于 s 个光子,他成功的概率仅为 $1/2^s$, s 为 Alice 选定的安全参数. 当 s 足够大时,Bob 作弊成功概率可以任意小.

3.2.2　交叉分组攻击

Bob 可以在 Step 5 中把跟 Alice 选择的基相同的那一组均匀地一分为二,然后把另一组也均匀地一分为二后附在这新的两组中. 这样,新的两组开头的$\lfloor N/2 \rfloor$个光子都是 Bob 所知道的正确结果,如果 Alice 选择的 n 小于$\lfloor N/2 \rfloor$,则 Bob 可以同时正确获得 b_0 和 b_1.

对抗这种欺骗方式的方法也很简单,只要保证 Alice 选择的 n 大于$\lfloor N/2 \rfloor$即可,对于较大的 N,这点是极为简单的. Bob 采取这种作弊手段的唯一结果就是 b_0 和 b_1 一个也得不到.

3.2.3　Breidbart 攻击

事实上,不诚实的 Bob 可以既不选择+ 基也不选择 × 基,而是选择最有利于他的正交基进行测量,这种攻击方式称为 Breidbart 攻击. 对于此种攻击方式,我们先考虑这种攻击方式的性能,再讨论协议的安全性.

定理 3　在 QOT(b_0, b_1)协议中,如果不考虑信道噪声,作弊的 Bob 至少可以获得 85% 光子比特的信息.

证明　如果不考虑信道噪声,对于诚实的 Bob,如果对于每个接收到的光子,采用的测量基与 Alice 的基相同,则肯定可以获得相同的比特信息;如果 Bob 测量基与 Alice 不同,则根据量子机制,他获得该光子比特的正确信息的概率是 50%. 所以,诚实的 Bob 可以以 75% 的正确率来获得全部光子的比特信息.

如果 Bob 作弊,即不采用标准的+ 基与 × 基进行测量,而是选择测量角度为 β 与 β+ 90°的正交基($\beta \in [0, \frac{\pi}{2}]$)来测量每一个光子,下面我们看看选择什么样的 β 可以使 Bob 最大限度地获得光子信息.

对于任意一个光子,如果它是 Alice 用+ 基测量的,那么 Bob 正确获得它的信息的概率是 $\cos^2\beta$;而如果是用 × 基测量的,则 Bob 正确获得它的信息的概率是 $\cos^2\left(\frac{\pi}{4}-\beta\right)$. 考虑到均匀随机性,Alice 选择两种加密基的概率是相等的,所以 Bob 正确获得每个光子比特信息的概率为

$$\Pr[c_i = \hat{c}_i] = \frac{1}{2}\cos^2\beta + \frac{1}{2}\cos^2\left(\frac{\pi}{4}-\beta\right) \qquad (1)$$

其中 c_i 与 $\hat{c}_i$ 分别表示 Alice 与 Bob 选择测量基后的测量结果.

为求得 $\Pr[c_i = \hat{c}_i]$ 的最大值,对函数 $f(\beta) = \frac{1}{2}\cos^2\left(\frac{\pi}{4}-\beta\right)$ 求一阶导,得:

$$f'(\beta) = -\frac{1}{2}\cdot 2\cos\beta\sin\beta - \frac{1}{2}\cdot 2\cos\left(\frac{\pi}{4}-\beta\right)\sin$$

$$\left(\frac{\pi}{4}-\beta\right)(-1)$$

$$=-\cos\beta\sin\beta+\cos\left(\frac{\pi}{4}-\beta\right)\sin\left(\frac{\pi}{4}-\beta\right) \quad (2)$$

令$f'(\beta)=0$, 易求得 $\beta=\frac{\pi}{8}$. 故当 $\beta=\frac{\pi}{8}$时, $\Pr[c_i=\hat{c}]$取最大值, 此时

$$\Pr[c_i=\hat{c}_i]=\frac{1}{2}\cos^2\frac{\pi}{8}+\frac{1}{2}\cos^2\left(\frac{\pi}{4}-\frac{\pi}{8}\right)$$

$$=\cos^2\frac{\pi}{8}\approx 0.85355>85\% \quad (3)$$

定理 3 证毕.

当然, 因为信道噪声的客观存在性, 这个最大值在实际中肯定还会小一些.

尽管从定理 3 可知, 不诚实的 Bob 最多可以获得超过 85% 的光子比特信息, 但对于他获得另外一个比特信息的贡献仍然是可忽略的, 对于此, 我们有 ——

定理 **4** Bob 即使使用 Breidbart 攻击, 也无法非法获得更多的比特信息.

略证: 同光子存储攻击一样, 如果没有引入承诺方案, Bob 最多可以以大约 85% 的概率同时获得 b_0 和 b_1, 但是因为需要在 Step4 中作出承诺, Bob 显然无法通过这一关. 可见, Breidbart 攻击也是行不通的.

4 结束语

较之经典环境下的 OT 协议, 本文的量子 OT 协议具有如下优点:

(1) 更高的安全性: 不对通信双方(甚至包括窃听的第三方) 的计算能力做任何假设, 因而协议是无条件安全或者说是信息论安全的.

(2) 有效的检测机制: 根据测不准原理与量子不可克隆定理, 任何窃听者都无所遁形 ——这在经典环境中几乎是不可能做到的.

(3) 更强的健壮性: 不对窃听者的信道做任何限制性假设, 即使存在窃听, 协议仍然有效. 同时也不依赖于任何可信或半可信的第三方.

由于本协议具有较好的安全性与较低的通信复杂度和计算复杂度, 除了可以用来构建密码学或安全多方计算其他的重要协议之外, 还可以推广到传送问题领域的其他计算模型中去, 例如秘密交换(Exchange of Secrets)、GOT(Generalized OT)、秘密的全或无揭露(All-or-Nothing Disclosure of Secrets) 等问题, 都可以归约为本文的 QOT(b_0, b_1) 协议.

在检测到窃听后, 使用 QPA 的方案可以有效纯化信道, 使 OT 协议继续进行, 但是效率会有一定程度的降低. 下一步的工作, 主要是研究效率更高的抗噪与抗窃听方案, 以及不用调用比特承诺方案的 QOT 协议.

参考文献:

[1] Michael O Rabin. How to exchange secrets with oblivious transfer[Z]. http://eprint.iacr.org/2005/187, Harvard University Technical Report 81, 1981.

[2] Shimon Even, Oded Goldreich, A Lempel. A randomized protocol for signing contracts[A]. Proc. CRYPTO'82[C]. New York: Plenum Press, 1983. 205-210.

[3] Claude Crépeau. Equivalence between two flavours of oblivious transfers[A]. CRYPTO'87[C]. Berlin Heidelberg: Springer, 1987.

[4] G Brassard, C Crépeau, Jearr Marc Robert. Information theoretic reductions among disclosure problems[A]. Proc the 27th IEEE Symposium on Foundations of Computer Science[C]. California: Springer-Verlag, 1986. 168-173.

[5] G Brassard, C Crépeau, Jearr Marc Robert. All-or nothing disclosure of secrets[A]. A M Odlyzko, editor, Proc CRYPTO'86[C]. Berlin Heidelberg: Springer-Verlag, 1987. 234-238.

[6] Christian Cachin. On the foundations of oblivious transfer[A]. Lecture Notes in Computer Science, Proceedings of EUROCRYPT'98[C]. Berlin Heidelberg: Spinger, 1998.

[7] Claude Crépeau. Efficient cryptographic protocols based on noisy channels[A]. Lecture Notes in Computer Science, Proceedings of EUROCRYPT'97[C]. Berlin Heidelberg: Springer, 1997. 306-317.

[8] RL Rivest. Unconditionally Secure Commitment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer[Z]. http://crypto.csail.mit.edu/~rivest/Rivest-commitment.pdf, 1999.

[9] Brassard G, Crépeau C, Wolf S. Oblivious transfers and privacy amplification[J]. Journal of Cryptology, 2003, 16(44): 219-237.

[10] Wolf S, Wullschleger J. Zero-Error Information and Applications in Cryptography[A]. Proceedings of 2004 IEEE Information Theory Workshop[C]. New York: IEEE, 2004. 1-6.

[11] Crépeau C, Kilian J. Achieving oblivious transfer using weakened security assumptions[A]. Proceedings of 29th IEEE Symposium on the Foundations of Computer Science[C]. New York: IEEE, 1988. 42-52.

[12] Brassard G, Crépeau C. Quantum bit commitment and coin tossing protocols[A]. Advances in Cryptology-Crypto'90 Proceedings[C]. Berlin Heidelberg: Springer-Verlag, 1991. 49-61.

[13] D Deutsch, A Ekert, R Jozsa, C Macchiavello, S Popescu, A Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels[J]. Phys Rev Lett, 1996, 77(13): 2818-2821.

[14] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Ueli M Maurer. Generalized privacy amplification[J]. IEEE Transac-

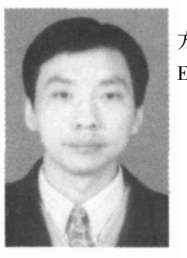
tions on Information Theory, 1995, 41(6): 1915- 1923.

[15] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Marie Helene Skubiszewska. Practical quantum oblivious transfer [A]. Advances in Cryptology-Crypto' 90 Proceedings[C]. Berlin Heidelberg: Springer-Verlag, 1991. 351- 366.

[16] Crépeau C. Verifiable disclosure of secrets and application [A]. Advances in Cryptology: Proceedings of Eurocrypt' 89 [C]. Berlin Heidelberg: Springer Verlag, 1989. 181- 191.

作者简介:

杨　威　男, 1978 年生于六安, 中国科学技术大学计算机科学与技术系博士. 研究方向为信息安全、量子信息.
E-mail: smartyw@mail.ustc.edu.cn



罗永龙　男, 1972 年生, 副教授, 博士, 研究方向为信息安全、分布式计算.
E-mail: yllluo@ustc.edu.cn

黄刘生　男, 1957 年生, 教授, 博士生导师, 研究方向为分布式计算、信息安全、无线传感网络. E-mail: lshuang@ustc.edu.cn

陈国良　男, 1938 年生, 中国科学院院士, 博士生导师, 研究方向为高性能计算.
E-mail: glchen@ustc.edu.cn

(上接第 1537 页)

[3] McKenna S etal. Tracking groups of people[J]. Computer Vision and Image Understanding, 2000, 80(1): 42- 56.

[4] G Doretto, A Chiuso, Y N Wu, S Soatto. Dynamic textures[J]. International Journal on Computer Vision (IJCV), 2003, 51(2): 91- 109.

[5] A Monnet, A Mittal, N Paragios, V Ramesh. Back-ground modeling and subtraction of dynamic scenes[A]. Proceedings of International Conference on Computer Vision(ICCV)[C]. Nice, France, 2003. 1305- 1312.

[6] J Zhong, S Sclaroff. Segmenting foreground objects from a dynamic textured background via a robust Kalman Filter[A]. Proceedings of International Conference on Computer Vision (ICCV)[C]. Nice, France, 2003. 44- 50.

[7] Wren C, Azarbayejani A, Darrell T. Pfinder. Real-time tracking of the human body[J]. IEEE Trans on Pattern Analysis and Machine Intelligence, 1997, 19(7): 780- 785.

[8] K Konolige. Small vision systems: Hardware and implementation [A]. Eighth Intl Symposium on Robotics Research[C]. Hayama, Japan, 1997. 111- 116.

[9] G Gordon, T Darrell, M Harville, Woodfill. Background estimation and removal based on range and color[A]. Proceedings of IEEE 1999 Computer Vision and Pattern Recognition (CVPR' 99)[C]. Ft. Collins, CO, USA, 1999. 459- 464.

[10] Gordon N J, Salmond D J, Smith A FM. Novel approach to nonlinear/ non-Gaussian Bayesian state estimation[J]. IEEE proceedings-F, 1993, 140(2): 107- 113.

[11] M Pitt, N Shepherd. Filtering via simulation: auxiliary particle filters[J]. Journal of American Statistical Association, 1999, 77(2): 590- 599.

[12] C Musso, N Oudjane, F LeGland. Improving Regularised Particle Filters[M]. Sequence Monte Carlo methods in practice, New York: Spring-Verlag, 2001.

[13] 陈坚, 王文成, 吴恩华. 单目视频中无标记的人体运动跟踪[J]. 计算机辅助设计与图形学学报, 2005, 17(9): 147- 153.
Chen Jian, Wang Wencheng, Wu Enhua. Markerless human motion tracking from monocular videos[J]. Journal of Computer-Aided Design & Computer Graphics, 2005, 17(9): 147- 153. (in Chinese)

[14] A Cavallaro, T Ebrahimi. Video object extraction based on adaptive background and statistical change detection[A]. Proceedings of SPIE Visual Communication and Image Processing [C]. San Jose, California, 2001. 4310. 465- 475.