高效短种子量子密钥分配保密放大方案设计

刘翼鹏[1]，郭建胜[1,2]，崔竞一[1]

[1]解放军信息工程大学三院，河南 郑州 450001；

[2]信息保障技术重点实验室，北京 100072

摘要 针对目前保密放大方案存在的随机种子使用量大的问题，提出了一种基于模块化广义 Trevisan 随机提取器结构的量子密钥分配(QKD)保密放大的设计方案，并借助量子边信息分析理论，给出了该方案的安全性证明。结果表明，该方案不仅能够抵抗量子攻击，而且能有效节约随机种子，实现可扩展的高效保密放大。

关键词 量子光学；量子密码；量子密钥分配；保密放大；广义 Trevisan 随机提取结构；种子伪随机扩展

中图分类号 TP309.7 **文献标识码** A

doi：10.3788/AOS201737.0227002

Scheme Design of Highly Efficient Privacy Amplification with Fewer Random Seeds in Quantum Key Distribution

Liu Yipeng[1], Guo Jiansheng[1,2], Cui Jingyi[1]

[1] *The Third Department, PLA Information Engineering University, Zhengzhou, Henan* 450001, *China;*

[2] *Science and Technology on Information Assurance Laboratory, Beijing* 100072, *China*

Abstract In consideration of the problem of the large usage of random seeds in the current privacy amplification schemes, one design scheme of privacy amplification in quantum key distribution (QKD) based on modular and generalized Trevisan's randomness extractor construction is proposed, and the confirmation of its security with the help of quantum side information analysis theory is presented. The results indicate that such a scheme not only resists against quantum attacks but also effectively reduces the usage of random seeds to ensure an efficient and malleable privacy amplification.

Key words quantum optics; quantum cryptography; quantum key distribution; privacy amplification; generalized Trevisan's randomness extractor construction; seed pseudorandom extension

OCIS codes 270.5568; 270.5585; 270.5565

1 引 言

量子密钥分配(QKD)是一种能够通过公开信道，在合法的通信双方 Alice 和 Bob 之间进行无条件安全密钥协同，从而获得一致秘密信息的方式[1-2]，它的安全性基于量子力学的基本原理。QKD 主要包括量子信号传输阶段和后处理阶段。量子信号传输阶段主要包括 Alice 和 Bob 之间进行的量子态发送、传输和测量的过程。后处理阶段主要包括基码和误码估计、密钥协商、错误校验及保密放大等过程[3-6]。后处理阶段是在可信的经典信道中进行的，攻击者只能窃听，但不能篡改其中的内容。由于在整个 QKD 过程中，Alice 和 Bob 相互通信的信息在一定程度上反映了密钥的性质，泄露了密钥的部分信息，因此在密钥协商与错误校验之后，需通过保密放大将这些泄露的信息去除。保密放大的主要目标是压缩冗余信息，从部分安全的密钥中提取出具有更高安全性的密钥[7]。

收稿日期：2016-08-16；**收到修改稿日期**：2016-10-08

基金项目：博士后科学基金(2014M562582)

作者简介：刘翼鹏(1992—)，男，硕士研究生，主要从事量子密码及量子随机数生成方面的研究。

E-mail：lyp_31@126.com

导师简介：郭建胜(1972—)，男，博士，教授，主要从事信息安全及密码理论方面的研究。

E-mail：tsg_31@126.com(通信联系人)

对于 QKD 的保密放大过程，公开的函数结构和相关信息都会对最终安全密钥的生成产生影响[8]。目前常用的是普适类哈希函数[9]，通信双方各有一个相同的可公开的哈希函数集，在进行保密放大的过程中，通过公开信道的通信，双方随机选取一个相同的哈希函数，将其作用到纠错后的密钥，从而获得最终的安全密钥。在保密放大过程中，需要一串随机数作为种子，以从哈希函数集中选取所需的哈希函数。然而，在目前的保密放大方案中，用于选取哈希函数的随机种子往往比输出密钥长，这既造成了资源的浪费，也会在一定程度上对 QKD 的安全性产生影响。因此，基于普适类哈希函数的保密放大存在真随机资源使用量大的缺点[10]。同时，攻击者可能拥有量子攻击能力。因此，设计能够抵抗量子攻击、并且对随机种子需求量少的高效保密放大方案，对提高 QKD 的安全性和实现效率都十分重要。

不同于基于普适类哈希函数的保密放大，本文将随机数提取器技术应用到 QKD 后处理环节中。随机数提取器是一类常用的从伪随机源中提取真随机数的工具。在各种随机数提取器结构中，基于纠错编码和伪随机数生成器理论的 Trevisan 随机提取结构是一类典型的强随机数提取器[11]，其具有随机种子使用量少、能抵抗量子攻击等特点[12]。强提取器的性质保证了 Trevisan 结构在提取过程中使用的随机种子与最终的输出序列是相互独立的，即种子可以重复使用。本文针对目前 QKD 后处理的保密放大环节中真随机资源使用量大的问题，利用 Trevisan 随机提取结构的构造思想，设计了广义 Trevisan 随机提取结构。该结构是抗量子攻击的、广义的、模块化的模型，可作为 QKD 的保密放大环节，其最大的特点是能有效减少真随机资源（种子）的使用量，并且能够保证保密放大环节在量子边信息下的安全性。基于上述对 QKD 保密放大环节的研究，综合考虑了实现效率和随机种子使用量，本文选用普适类哈希函数作为子提取模块，结合种子伪随机扩展算法，设计了一种基于广义 Trevisan 随机提取结构模型的高效短种子 QKD 保密放大方案。在输入长度为 n 的情况下，其计算复杂度为 $O(n\mathrm{lb}\ n)$，种子使用量为 $O(\mathrm{lb}\ n)$，并在量子边信息分析理论[13]下对该方案的安全性进行了全面分析。

2　基础知识

QKD 的后处理环节在安全密钥的生成过程中是十分重要的，主要包括基码和误码估计、密钥协商、错误校验及保密放大过程[7]，如图 1 所示。

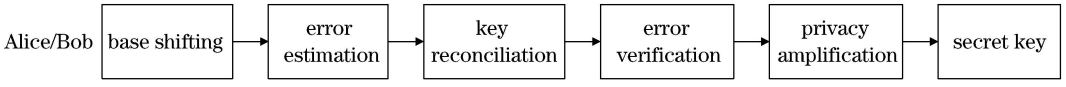

图 1　QKD 后处理过程的流程图

Fig. 1　Flow chart of post-processing procedure in QKD

本文重点研究后处理环节中的保密放大部分，对于量子信号传输阶段以及基码和误码估计等不作重点讨论。

2.1　保密放大

由于在纠错过程中，通信双方相互通信的信息在一定程度上泄露了密钥的信息量，因此在提取安全密钥时需要将这些泄露的信息量去掉[14-15]。保密放大就是通过压缩冗余信息，使得通信双方最终获得一致的安全密钥。

目前主要利用基于 Toeplitz 矩阵[16-17]、模算术[13]及有限域乘法[15,17]的普适类哈希函数[14-15]来实现保密放大。通常情况下，保密放大过程是在纠错过程之后进行的，但是也可以在一次一密加密过程之后进行，即直接使用纠错后的密钥来对需要传送的信息进行一次一密加密，之后再进行保密放大[18]。

2.2　Trevisan 随机提取结构

通常利用小熵来衡量从伪随机源中提取的最大真随机数。对于随机变量 X，其概率 P 的取值空间为 χ，则其小熵为 $H_{\min}(X)=-\mathrm{lb}[\max P(x),x\in\chi]$。当随机变量 X 呈均匀分布时，其熵达到最大。在实际情况中，由于随机源可能存在一定的信息泄露，其相应的随机变量的熵不能达到所在空间的最大熵，而随机源能够达到的最大熵就是小熵。

利用随机数提取器可以从伪随机源中提取真随机数。对于一个 (k,ε) 提取器（$0\leqslant k\leqslant n$，提取器偏差

$\varepsilon \geqslant 0$)，当其输入的伪随机源的小熵不小于 k 时，其输出序列与真随机数之间的统计距离不大于 ε。当输出序列与随机种子之间相互独立时，即种子可以重复使用，则称之为强提取器。2000 年，Trevisan[11] 提出利用 Nisan-Wigderson 伪随机数生成器[19]和一类纠错编码(可列可解码)构造随机数提取器，证明了在弱随机资源具有足够大的小熵[20]情况下，随机挑选此类纠错编码一个输出位置的比特，该比特是接近真随机的。在 Trevisan 随机提取结构中，随机种子就是用来确定纠错编码输出位置的。因此，如果输出比特链的编码长度为 $L'=\mathrm{poly}(L)$，则只需要长度为 $\mathrm{lb}\ L'$ 的种子，其中 L 为输入的伪随机源的长度。相比其他提取器，Trevisan 随机提取结构需要的种子长度相对较短。

同时，Trevisan 也利用其提出的一比特提取器构造了一类多比特提取器，证明了在伪随机源的小熵满足一定条件的情况下，1 bit 级联产生的多比特输出是接近真随机的[11]。为了使用更少的种子，Trevisan 在构造多比特提取器时利用了 Nisan 等[19]提出的交集结构。其基本思想是将最初的随机种子分成若干个有一定重叠的集合，如果重叠度不是很大，那么级联产生的多比特输出之间的相关性较小，利用最初弱随机资源的随机性便可将这些相关性消除。这种将种子分成一些小集合交集的方法经 Ran 等[21]改进后，拥有了更好的性质，此类方法统称为弱设计，即

定义 1[21]：如果一个集合族 $S_1,\cdots,S_m\subset\{1,\cdots,D\}$，且当 $i=1,\cdots,m$ 时，$|S_i|=t$，$\sum_{j=1}^{i-1}2^{|S_j\cap S_i|}\leqslant rm$，则该集合族称为($t$，$r$)弱设计。其中 r 为种子弱设计的重叠度，m 为比特数，D 为整数。

结合弱设计，Trevisan 随机提取结构可以描述为如下定义 2。

定义 2[22]：对于一个种子长度为 t 的一比特提取器 $C:\{0,1\}^n\times\{0,1\}^t\to\{0,1\}$，以及一个($t$，$r$)弱设计，定义 m 比特提取器为 $E_{xtC}(x,y)=C(x,y_{S_1})\cdots C(x,y_{S_m})$，其中 x、y 为序列，y_{S_i} 为序列 y 中由 S_i 集合确定的位置的比特。Trevisan 提取器结构框图如图 2 所示。

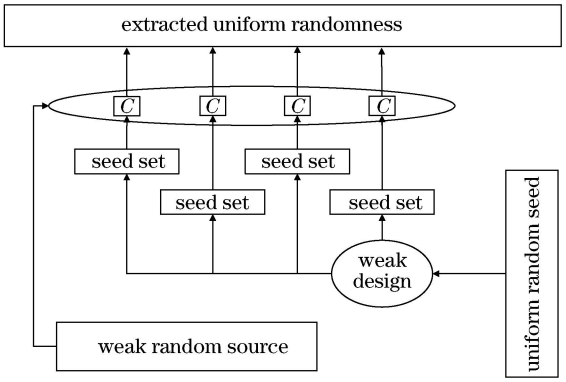

图 2　Trevisan 提取器结构框图

Fig. 2　Block diagram of Trevisan's extractor construction

Trevisan 提取器之所以引起广泛兴趣，主要有三个原因。第一，其能抗量子攻击。在 Konig 等[23]证明的基础上，De 等[12]给出了 Trevisan 结构在量子边信息下的安全性参数，即 Trevisan 结构为量子边信息下的$[k+rm+\mathrm{lb}(1/\varepsilon),3m\sqrt{\varepsilon}]$强提取器，这说明当输入伪随机源在量子边信息下的条件小熵不小于 $k+rm+\mathrm{lb}(1/\varepsilon)$时，Trevisan 提取器的输出与真随机数之间的统计距离不大于 $3m\sqrt{\varepsilon}$，且输出独立于随机种子和量子边信息。第二，Trevisan 随机提取结构的真随机种子使用量很少，在实际应用过程中能较好地节约资源。第三，Trevisan 随机提取结构为强提取器，其种子和输出比特之间是相互独立的，即种子可以重复使用，此性质保证了其应用在 QKD 保密放大环节的可行性。基于 Trevisan 随机提取结构的上述优点，本文将其模块化，给出基于广义 Trevisan 随机提取结构的保密放大模型，并分析其在量子边信息分析理论下的安全性。

3　基于广义 Trevisan 随机提取结构的保密放大模型

QKD 保密放大环节的重点是去除攻击者拥有的关于密钥的信息量。一般以普适类哈希函数作为密钥，使哈希函数的输出长度小于攻击者的不确定度。对于利用哈希函数进行保密放大的方法，通信双方需要共

享一个随机值以从哈希函数族中选取本次通信使用的哈希函数，并且此随机值是可以在公开信道中传输的。设经过纠错后通信双方得到长度为 n bit 的密钥，经过计算，其最终的安全密钥长度为 m bit，那么实现保密放大一般需要随机选取一个 $m\times n$ 维的二进制矩阵，将纠错后的密钥与该矩阵作用后得到长度为 m bit 的安全密钥。但在实际应用中，每进行一次保密放大，就需要在公共信道中传输（$m\times n$）bit 的数据（称为种子），不利于大量数据处理。Toeplitz 矩阵[9-10]的运用使得仅需要（$n+m-1$）bit 随机数便可描述矩阵，但公共传输的随机数据依然大于最终的密钥生成量。通信双方公开传输的信息越多，保密放大过程的信息泄露就会越多。因此，减少保密放大过程中公开传输的随机数据是至关重要的。

由前面的分析可知，Trevisan 随机提取结构是一类强提取器，种子使用量仅为输入序列长度的多重对数，并且种子与输出值之间相互独立，种子可以重复利用。因此，利用 Trevisan 提取结构作用通信双方经密钥协商后的值，在减少种子使用量的同时，可以有效压缩密钥的冗余信息，获得最终安全密钥；其强提取器的性质也保证了种子可以在可信的公开信道中传输。在 QKD 的整个过程中，攻击者可能拥有量子攻击能力，因此在量子边信息下考虑最终密钥的安全性是必要的，具有抗量子攻击特性的 Trevisan 结构很好地解决了这个问题。

与普适类哈希函数不同，Trevisan 随机提取结构的输出是由若干个一比特提取器级联组成的，且每比特输出都是随机的。更关键的是，它的构造方法决定了其输出长度都小于伪随机源的条件小熵，这也保证了最后提取得到的密钥的安全性。

基于 Trevisan 随机提取结构的优势及其在量子边信息分析理论下的安全性结论，将 Trevisan 随机提取结构模块化后推广到更一般的情况，并运用到 QKD 的保密放大环节；设计一种基于广义 Trevisan 随机提取结构的保密放大模型，并给出其在量子边信息下的安全性证明。

3.1　基于广义 Trevisan 随机提取结构的保密放大模型

由 2.2 节中的分析可知，Trevisan 随机提取结构的输入分为伪随机源和经弱设计处理后的种子。弱设计将初始的随机种子扩展到多个种子集合，每个集合之间存在一定的重叠度，从而使种子的总长度满足提取器的使用要求。Trevisan 结构在每一次提取过程中，每个一比特提取器均输入相同的伪随机源和经弱设计处理后的不同种子集合，然后将其输出的 1 bit 级联，得到最后的随机数。

基于 Trevisan 结构的构造思想，将 Trevisan 随机提取结构模块化，对各个部分给出更广义的定义。模块化的 Trevisan 结构可以分为种子预处理模块和子提取模块两部分。初始随机种子经过种子预处理模块的作用后，将其输入到子提取模块中，最终获得随机数。由于 Trevisan 结构为强提取器，其种子独立于输出的随机数，因此，在 QKD 的后处理过程中，通信双方可以通过公开可信信道传输随机种子。通信双方首先共享一串较短的随机种子，然后将种子和纠错后的密钥输入到广义 Trevisan 随机提取结构中，得到最终安全密钥。基于广义 Trevisan 随机提取结构的 QKD 保密放大模型如图 3 所示。

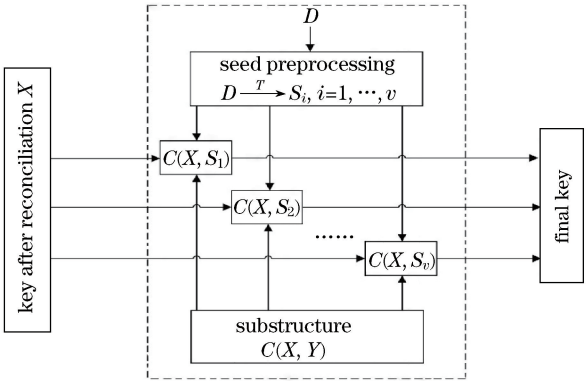

图 3　基于广义 Trevisan 随机提取结构的保密放大模型

Fig. 3　Model for privacy amplification based on generalized Trevisan's randomness extractor construction

图 3 中的保密放大模型具体描述如下。

模型 1：1）Alice 和 Bob 经过量子信号传输、基数和参数估计、密钥协商及错误校验过程，获得相同的密

钥 X；2）Alice 和 Bob 计算出欲提取的安全信息量 m，并通过可信信道共享一串长为 D 的随机种子 Y；3）Alice和 Bob 利用种子预处理模块 T 处理共享的随机种子 Y，从而得到 v 个种子集合 S_i，$i=1,\cdots,v$；4）Alice和 Bob 选择相同的子提取模块，将密钥 X 和种子集合 S_i 输入到子提取模块中，每次更换一个 S_i，经过 v 次作用，最终得到 m 的安全密钥 $Z=C(X,S_1)\cdots C(X,S_v)$。

在上述模型 1 中，初始随机种子 Y 的长度 D 是由通信双方使用的子提取模块的种子长度、种子预处理模块以及保密放大最终产生的安全密钥长度共同决定的。

以原始的 Trevisan 结构为例，其种子预处理模块为弱设计结构，子提取模块为一比特提取器。原始 Trevisan 结构的本质是先利用可列可解码[24]对输入比特进行编码，然后从编码序列中随机选取 1 bit，因此在输入伪随机源具有一定小熵的条件下，选取的 1 bit 是接近真随机的。利用 Alice 和 Bob 通过可信信道共享的一串随机种子，可从编码序列中随机选取输出比特。因此，如果 n 为经纠错后的密钥长度，经可列可解码编码后的密钥长度为 $n'=\mathrm{poly}(n)$，那么仅需要长为 $\mathrm{lb}\ n'$ 的随机值即可完成选取，即在公共信道中传输的随机种子仅为输入值的多重对数。由 Ran 等[21]的研究可知，在一般情况下，当弱设计的重叠度 $r=2\mathrm{e}$ 时，$d=t^2$；当 $r=1$ 时，$d=at^2$，其中 e 为自然底数，t 为一比特提取器所需种子长度，$a=\left[\dfrac{\mathrm{lb}(m-2\mathrm{e})-\mathrm{lb}(t-2\mathrm{e})}{\mathrm{lb}(2\mathrm{e})-\mathrm{lb}(2\mathrm{e}-1)}\right]$。而最终安全密钥长度则由在保密放大步骤前对信道的估计以及密钥协商步骤中泄露的比特数决定。因此，如果使用弱设计和一比特提取器构造保密放大方案，其随机种子的使用量约为 $D=O(t^2\mathrm{lb}\ m)\approx O(\mathrm{lb}^3 n)$。目前 QKD 协议的后处理环节多用哈希函数，但哈希函数有随机种子使用量大[约为 $O(n)$]的缺点[10-11]。显然，当处理数据的长度 n 较大时，Trevisan 随机提取结构的真随机种子使用量远小于哈希函数，即 $O(\mathrm{lb}^3 n)<O(n)$。因此，基于广义 Trevisan 随机提取结构的 QKD 保密放大模型的保密放大方案可以有效减少通信双方随机种子的使用量。

3.2　安全性分析

2005 年，Renner[20]提出了基于量子信息论的 QKD 安全证明思想，并给出两个安全参数 $\varepsilon_{\mathrm{cor}}$（一致性参数）和 $\varepsilon_{\mathrm{sec}}$（保密性参数）。保密性参数 $\varepsilon_{\mathrm{sec}}$ 是描述 QKD 最终的安全密钥至少以 $1-\varepsilon_{\mathrm{sec}}$ 的概率与无量子攻击条件下的密钥是相同的，即经保密放大后通信双方的安全密钥 Z 与真随机数 U_Z 之间的统计距离满足

$$\|\rho_{ZE}-U_Z\otimes\rho_E\|\leqslant\varepsilon_{\mathrm{sec}},\tag{1}$$

式中 ρ_E 是攻击者 Eve 拥有的量子系统，ρ_{ZE} 是 Z 和 ρ_E 的经典-量子态（cq-态），U_Z 是关于 Z 所有取值的单位矩阵。

与普适类哈希函数不同，Trevisan 随机提取结构的安全性证明最早是基于纠错编码和伪随机数生成器理论给出的，后来考虑到量子边信息的影响，De 等[12]给出了其抗量子攻击的安全性证明。由于在 QKD 的整个过程中，攻击者可能拥有量子攻击能力，因此对于基于广义 Trevisan 随机提取结构的 QKD 保密放大模型来说，需要在量子边信息下讨论其安全性。

结合原始 Trevisan 随机提取结构在量子边信息分析理论下的安全性结论可知[8]，对于基于广义 Trevisan 随机提取结构的 QKD 保密放大模型，如果经种子预处理后的种子集合之间的相关性不大，则当输入伪随机源具有足够大的小熵时，输出序列以很大的概率接近真随机数。基于上述分析，给出基于广义 Trevisan 随机提取结构的 QKD 保密放大模型在量子边信息下的安全性分析。

首先给出如下引理 1[23]。

引理 1：考虑一个 cccq-态 ρ_{XVWQ}，其中 ρ 表示系统的量子态，Q 表示量子系统，V、W、X 表示经典系统，$\rho_{XV}=\rho_X\otimes\rho_V$ 并且 $VW\leftrightarrow X\leftrightarrow Q$ 形成一个马尔科夫链，那么

$$H_{\min}(X\,|\,VWQ)\geqslant H_{\min}(X\,|\,Q)-H_0(W),\tag{2}$$

式中 $H_{\min}$ 表示小熵，$H_0(W)=\mathrm{lb}\,|\,supp(P_W)\,|$，$supp(P_W)=\{w:P[W=w]>0\}$。同时，以不小于 $1-\varepsilon$ 的概率有

$$H_{\min}(X\,|\,V=v,W=w,Q)\geqslant H_{\min}(X\,|\,Q)-H_0(W)-\mathrm{lb}(1/\varepsilon)。\tag{3}$$

结合引理 1 以及 Trevisan 结构的相关结论，可得模型 1 的安全性参数，即

定理 2：设模型 1 中子提取模块 $C(x,y)$ 为量子边信息下的 (k,ε) 强提取器，其输出长度为 l。Y 经种子

预处理模块后得到种子集合 $S_i(i=1,\cdots,\nu)$，设 $H_0(T)=\max[I(S_i;S_1,\cdots S_{i-1},S_{i+1},\cdots,S_\nu)]$，则广义 Trevisan 随机提取结构构成一个量子边信息下的$[k+l\nu+H_0(T)+\mathrm{lb}(1/\varepsilon),2\nu\varepsilon]$强提取器。

由模型 1 可知

$$Z=C(x,S_1)\cdots C(x,S_m), \tag{4}$$

设

$$\rho^{(i)}=\rho_{U_{\{0,1\}^l}}^{\otimes\nu-i}\otimes\rho_Y\otimes\rho_{z^iQ}, \tag{5}$$

$$z^i=C(x,S_1)\cdots C(x,S_i), \tag{6}$$

则

$$\rho^{(0)}=\rho_{U_{\{0,1\}^l}}^{\otimes\nu}\otimes\rho_Y\otimes\rho_Q, \tag{7}$$

$$\rho^{(\nu)}=\rho_Y\otimes\rho_{ZQ}。 \tag{8}$$

由三角不等式可得

$$\|\rho^{(\nu)}-\rho^{(0)}\|=\Big\|\sum_{i=0}^{\nu-1}\rho^{(i+1)}-\rho^{(i)}\Big\|\leqslant\sum_{i=0}^{\nu-1}\|\rho^{(i+1)}-\rho^{(i)}\|=$$

$$\sum_{i=0}^{\nu-1}\|\rho_{C(x,S_{i+1})z^iYQ}-\rho_{U_{\{0,1\}^l}}\otimes\rho_{U_Y}\otimes\rho_{z^iQ}\|, \tag{9}$$

设

$$\alpha=\|\rho_{C(x,S_{i+1})WQ}-\rho_{U_{\{0,1\}^l}}\otimes\rho_{U_Y}\otimes\rho_{WQ}\|, \tag{10}$$

则有

$$\alpha=\underset{W\leftarrow P_W}{E}\|\rho_{C(x,S_{i+1})W=w,Q}-\rho_{U_{\{0,1\}^l}}\otimes\rho_{U_Y}\otimes\rho_{W=w,Q}\|, \tag{11}$$

式中 W 代表 $S_1,\cdots,S_i,S_{i+2},\cdots,S_\nu$ 和 z^i 中与 $C(x,S_{i+1})$ 相关的信息。因为 $H_0(W)\leqslant H_0(z^i)+H_0(T)\leqslant l\nu+H_0(T)$，由引理 1 可知，以不少于 $1-\varepsilon$ 的概率满足

$$H_{\min}(X|W=w,Q)\geqslant k。 \tag{12}$$

又因为 $C(x,y)$ 为量子边信息下的(k,ε)强提取器，所以对于任意的 W，有

$$\|\rho_{C(x,S_{i+1})W=w,Q}-\rho_{U_{\{0,1\}^l}}\otimes\rho_{U_Y}\otimes\rho_{W=w,Q}\|\leqslant\varepsilon, \tag{13}$$

故 $\alpha\leqslant2\varepsilon$，进而可得

$$\|\rho^{(\nu)}-\rho^{(0)}\|\leqslant2\nu\varepsilon。 \tag{14}$$

由定理 1 可知，当输入伪随机源的条件小熵不小于 $k+l\nu+H_0(T)+\mathrm{lb}(1/\varepsilon)$ 时，输出序列以很大的概率接近真随机数。因此基于模型 1 的 QKD 处理后的保密性参数 $\varepsilon_{\mathrm{sec}}$ 满足定理 3。

定理 3：如果基于广义 Trevisan 随机提取结构的 QKD 保密放大模型（模型 1）构成一个量子边信息下的(k,ε)强提取器，则其保密性参数 $\varepsilon_{\mathrm{sec}}=\varepsilon$。

假设基于广义 Trevisan 随机提取结构的 QKD 保密放大模型构成一个量子边信息下的(k,ε)强提取器，则当经纠错后的密钥满足 $H_{\min}(X|E)_\rho\geqslant k$ 时，最终密钥满足

$$\|\rho_{E_{xt}(X,Y)YE}-\rho_{U_m}\otimes\rho_Y\otimes\rho_E\|\leqslant\varepsilon, \tag{15}$$

即保密性参数 $\varepsilon_{\mathrm{sec}}=\varepsilon$。

由定理 2 可知，如果将原始的 Trevisan 随机提取结构用于模型 1 中，其保密性参数 $\varepsilon_{\mathrm{sec}}=3m\sqrt{\varepsilon}$，其中 ε 为 1 bit 提取的参数。

在保密放大过程中，如果采用广义 Trevisan 随机提取结构，则在随机种子公开和攻击者拥有量子边信息的条件下，安全密钥的信息熵满足如下定理 4。

定理 4：设经过基于广义 Trevisan 随机提取结构的 QKD 保密放大过程后的密钥为 $Z=E_{xt}(X,Y)$，$Z\in\{0,1\}^m$，且其保密性参数为 $\varepsilon_{\mathrm{sec}}$，则安全密钥 Z 的条件信息熵满足 $H(Z|QY)\geqslant m-m\sqrt{\varepsilon_{\mathrm{sec}}}-O(\varepsilon_{\mathrm{sec}})$。

由定理 3 可知，当 $H_{\min}(X|E)_\rho\geqslant k$ 时，有

$$\|\rho_{E_{xt}(X,Y)YE}-\rho_{U_m}\otimes\rho_Y\otimes\rho_E\|\leqslant\varepsilon_{\mathrm{sec}}, \tag{16}$$

则以不小于 $1-\sqrt{\varepsilon_{\mathrm{sec}}}$ 的概率有

$$\left\|\rho_{E_{xt}(X,Y=y)YE}-\rho_{U_m}\otimes\rho_{Y=y}\otimes\rho_E\right\|\leqslant\sqrt{\varepsilon_{\mathrm{sec}}},\tag{17}$$

因此 $H(Z|QY=y)\geqslant m-O(\varepsilon_{\mathrm{sec}})$。故

$$H(Z|QY)\geqslant m-m\sqrt{\varepsilon_{\mathrm{sec}}}-O(\varepsilon_{\mathrm{sec}})。\tag{18}$$

设 $I(A;B)$为 A 与 B 之间的互信息，根据互信息的定义，有

$$I(Z;QY)=H(Z)-H(Z|QY),\tag{19}$$

式中 $H(Z)=m$。由定理 4 可得

$$I(Z;QY)\leqslant m\sqrt{\varepsilon_{\mathrm{sec}}}+O(\varepsilon_{\mathrm{sec}}),\tag{20}$$

式中 $I(Z;QY)$即为经保密放大后攻击者可以获取的信息量，$m\sqrt{\varepsilon_{\mathrm{sec}}}+O(\varepsilon_{\mathrm{sec}})$为其窃取信息量的上限。

4　高效短种子 QKD 保密放大方案设计及其安全性分析

在实际应用过程中，模型 1 的种子预处理模块和子提取模块不限于弱设计结构和一比特提取器。模型 1 不仅仅是一种算法，更是一种广义的保密放大构造方法。考虑保密放大的实现效率、随机种子的使用量等因素，通信双方可以利用不同的算法来实现保密放大。

经过第 3 节的分析可知，将基于弱设计和一比特提取器的 Trevisan 随机提取结构用于 QKD 的保密放大环节可以有效减少随机种子的使用量。然而在实际应用中，随机种子的获得往往较为困难，为了提高 QKD 系统的安全性，通信双方希望尽可能减少在公开信道上的信息交流，因此，更大程度地降低保密放大种子的使用量是必要的。同时，实际 QKD 的效率往往受限于后处理过程，因此在基于广义 Trevisan 随机提取结构的保密放大模型中，降低子提取模块的计算复杂度、提高输出速率是必要的。

4.1　种子的伪随机扩展

弱设计是目前 Trevisan 随机提取结构中最常使用的种子处理结构，其参数 t 由使用的一比特提取器决定，重叠度 r 由不同一比特提取器种子集合的交集确定。尽管使用了 Nisan 和 Wigderson 的种子处理方法，在一定程度上缩短了种子的长度，但是由于 Trevisan 结构要求每个一比特提取器输入种子之间的相关性尽量小，因此不同种子之间的重叠度也必须减小，而缩小重叠度必然导致初始随机种子长度的增加。提取结构输入种子的长度与 t 成正比、与 r 成反比，要实现接近完美的重叠度($r=1$)，不仅会使初始随机种子的使用量大幅度增加，而且会使相应的弱设计结构变得较为复杂[22]。

伪随机变换具有变换前后输入与输出之间相关性很小的特点，如果使用安全高效的伪随机变换对预置的短随机种子进行扩展处理得到更长的伪随机种子，再将扩展后的种子分组应用于一比特提取器，则既可以满足提取器的需要，又可以有效减少初始随机种子的需求量，同时也能够提高安全性。在实际应用中，为了提高种子预处理模块的工作效率，选用功耗低的轻量级分组密码算法来对初始随机种子进行伪随机扩展。

设 $f(x)$为一个轻量级分组密码，分组长度为 T，密钥长度为 K，预置的随机种子长度为 D，随机提取结构的输出长度为 m，则具体的种子扩展算法如下，记为算法 1，即

第一步：将长度为 D 的真随机种子分为 $m_1=\lfloor D/t\rfloor$组，每组长为 t(t 为子提取模块所需种子长度)，记为 $y_1,\cdots,y_{m_1}$，作为种子输入子提取模块。

第二步：使用完预制的 D 真随机种子后，利用轻量级分组密码算法 $f(x)$对随机种子进行扩展，将 D 真随机种子分成 $l'=\lceil D/t\rceil$组，每组长为 T，记为 $y'_1,\cdots,y'_{l'}$，不足的采用随机数挪用的方法来进行尾分组处理，利用密钥 K 分别对每组进行加密，加密后的种子集合为 $f(y'_1,K),\cdots,f(y'_{l'},K),f^2(y'_1,K),\cdots,f^2(y_{l'},K)\cdots$。

第三步：利用轻量级分组密码将算法加密后的伪随机种子分组(每组长为 t)用于随机提取结构，提取(m-m_1) bit 随机数后，更换密码算法的密钥，重复第二步，继续对随机种子进行扩展，用于后续随机数的提取。

利用上述伪随机扩展算法，避免了弱设计结构中的比特重用问题。相比之下，要使弱设计的重叠度达到 1，初始随机种子的长度 $D=O(t^2\mathrm{lb}\ m)\approx O(\mathrm{lb}^3 n)$。而在种子伪随机扩展处理过程中，当加密算法保证足够

的安全性时，预置的随机种子长度甚至可以减小到子提取模块的种子需求量，一般仅需要 $D=O(t)\approx O(\mathrm{lb}\ n)$。

4.2　高效短种子保密放大方案

一比特提取器的子提取模块存在计算复杂度相对较大的缺点，并受限于 1 bit 输出结构，提取速率较慢。虽然 Mauerer 等[22]通过替换基于纠错编码的一比特提取器来提高提取速率，但依然受 1 bit 结构自身的限制。

首先简单介绍普适类哈希函数。

定义 3[25]：普适类哈希函数族 H 是从集合 A 到集合 B 的映射，如果对于任意的 $x\neq y\in A$，$P_{h\in H}\{h(x)=h(y)\}\leqslant 1/|B|$，则哈希函数族 H 称为普适类哈希函数族，其中 $|B|$ 表示集合 B 中元素的数目。

在保密放大过程中，随机种子需要公开，且一般情况下用来构造 Toeplitz 矩阵的随机种子比最终输出值要长，因此需要种子可以重复使用，即要求普适类哈希函数族为强提取器。

定理 5[25]：设 $H=\{h_1,h_2,\cdots,h_{2^D}\}$ 为从 $\{0,1\}^n$ 映射到 $\{0,1\}^s$ 的普适类哈希函数族，G 为 $\{0,1\}^n$ 上的概率分布，且 $H_{\min}(G)\geqslant k$，则对于 $g\in G$，$h_y\in H(y\in U_D)$，$h_y(g)$ 与 y 的级联和 U_{m+D} 之间的统计距离不大于 $\varepsilon=2^{(s-k)/2}$，即此过程形成了一个 $[k,2^{(s-k)/2}]$ 强提取器。

由定理 5 可知，用于构造 Toeplitz 矩阵的随机种子在 QKD 保密放大环节可以重复使用。由于 Toeplitz 哈希函数的计算复杂度相对较低，且输出长度不局限于 1 bit 结构，因此这里使用 Toeplitz 哈希函数作为子提取模块，同时结合算法 1 扩展后的种子集合，给出基于模型 1 的高效短种子保密放大方案 1，如图 4 所示。

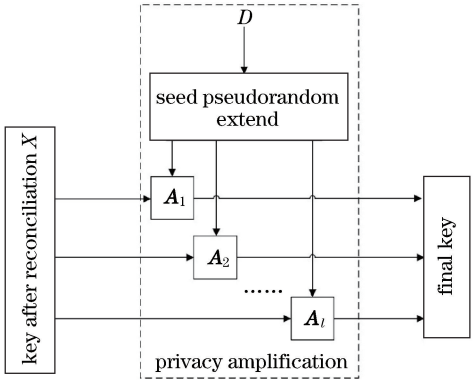

图 4　高效短种子保密放大方案示意图

Fig. 4　Schematic diagram of highly efficient privacy amplification with less random seeds

方案 1 具体如下。

第一步：Alice 和 Bob 经过量子信号传输、对基、参数估计、密钥协商和错误校验过程，获得相同的密钥 X。

第二步：Alice 和 Bob 计算出欲提取的安全信息量 m，并通过可信信道共享一串长度为 D 的随机值 Y。

第三步：Alice 和 Bob 利用伪随机扩展算法（算法 1）将长度为 D 的随机值进行扩展，得到扩展后长度为 d 的种子。

第四步：利用扩展后的种子构造 Toeplitz 矩阵，设哈希函数的输出长度为 s，则共需构造 $l=(m/s)$ 个 Toeplitz 矩阵 $\boldsymbol{A}_i(i=1,\cdots,l)$，每个矩阵构造需要 $(n+s-1)$ 个扩展后的种子。

第五步：利用已构造的 l 个 Toeplitz 矩阵与初始数据相互作用，最终获得安全密钥。

由算法 1 的分析可知，方案 1 所用的种子经伪随机扩展方法获得，因此仅需要 $D=O(t)\approx O(\mathrm{lb}\ n)$。方案 1 需要进行 l 次 Toeplitz 矩阵的乘法运算，使用快速傅里叶变换可将方案 1 计算复杂度降低到 $O(n\mathrm{lb}\ n)$。

4.3　高效短种子保密放大方案的安全性分析

Bertar 等[13]结合算子空间理论，给出了提取器在量子边信息下的相关结论，即

定理 6[13]：设 $C:\{0,1\}^n\times\{0,1\}^t\rightarrow\{0,1\}^l$ 为 (k,ε) 强提取器，则 C 为量子边信息下的 $[k+\mathrm{lb}(2/\varepsilon),c\sqrt{2^l}\sqrt{2\varepsilon}]$ 强提取器，其中 c 为参数。

由定理 5 和定理 6 可知，从$\{0,1\}^n$映射到$\{0,1\}^s$的普适类哈希函数族$H=\{h_1,h_2,\cdots,h_{2^D}\}$构成一个量子边信息下的$[k+\mathrm{lb}(2/\varepsilon),c\sqrt{2^{(3s-k)/2+1}}]$强提取器。

基于定理 2、定理 5 以及定理 6，可得如下定理 7。

定理 7：设$H=\{h_1,h_2,\cdots,h_{2^D}\}$为从$\{0,1\}^n$映射到$\{0,1\}^s$的普适类哈希函数族，种子伪随机扩展所用的变换为$f(x)$，则方案 1 中的保密放大过程$E(x,D)=h_{S_1}\cdots h_{S_l}$($S_1,\cdots,S_l$为经伪随机扩展后的种子集合)构成了一个量子边信息下的$\{k+m+K+2\mathrm{lb}(2/\varepsilon),l\cdot[c\sqrt{2^{(3s-k)/2+1}}+2^{(s-k)/2}]\}$强提取器，其中$K$为算法 1 中所用轻量级分组密码算法的密钥长度。

由定理 7 可知，方案 1 的保密性参数为$\varepsilon_{\mathrm{sec}}=l\cdot[c\sqrt{2^{(3s-k)/2+1}}+2^{(s-k)/2}]$。相比于一般的基于普适类哈希函数的保密放大，方案 1 在节约随机种子使用量方面有一定的优势，结果见表 1。

表 1　保密放大相关结果比较

Table 1　Comparison among privacy amplification results

Structure	Complexity	Seed length	Secrecy
Two-universal hash function	$O(n\mathrm{lb}\,n)$	$O(n)$	$O(\sqrt{2^m\sqrt{\varepsilon}})$
Trevisan's construction	poly(n)	$O(\mathrm{lb}^3 n)$	$O(m\sqrt{\varepsilon})$
Scheme 1	$O(n\mathrm{lb}\,n)$	$O(\mathrm{lb}\,n)$	$O(\sqrt{2^m\sqrt{\varepsilon}})$

分析结果表明，方案 1 不仅能够抵抗量子攻击，而且能节约随机种子、实现可扩展的高效保密放大。

5　结　论

通过对现有保密放大方案优缺点的深入研究，针对目前存在的随机种子使用量大的问题，将 Trevisan 随机提取结构模块化，并应用到 QKD 的保密放大环节。提出了一种新型的、可扩展的基于广义 Trevisan 随机提取结构的 QKD 后处理模型，有效减少了保密放大环节中真随机数的使用量。建立了保密放大方案保密性参数与随机提取结构安全参数之间的关系，给出了经保密放大模型作用后攻击者窃取信息量的上界。基于提出的保密放大模型，综合考虑实现效率和随机种子的使用量，结合普适类哈希函数和种子伪随机扩展思想，利用轻量级分组密码算法扩展随机种子，设计了一种能够抵抗量子攻击的高效短种子 QKD 保密放大方案。在输入长度为n的情况下，其计算复杂度为$O(n\mathrm{lb}n)$，种子使用量为$O(\mathrm{lb}n)$。

基于广义 Trevisan 随机提取结构的保密放大模型是一种模块化的、可扩展的、灵活的模型，在实际应用中，针对不同的需求，可以选择不同的模块算法，从而达到更好的保密放大效果。

参　考　文　献

[1] Shannon C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[2] Bennet C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing[J]. Theoretical Computer Science, 2014, 560(1): 7-11.

[3] Li M, Patcharapong T, Zhang C M, *et al*. Efficient error estimation in quantum key distribution[J]. Chinese Physics B, 2015, 24(1): 010302.

[4] Dou Lei, Guo Dabo, Wang Xiaokai. Optimizing multidimensional reconciliation algorithm for continuous-variable quantum key distribution[J]. Acta Optica Sinica, 2016, 36(9): 0927001.
窦　磊, 郭大波, 王晓凯. 连续变量量子密钥分发多维数据协调算法优化[J]. 光学学报, 2016, 36(9): 0927001.

[5] Zhang C M, Li M, Huang J Z, *et al*. Fast implementation of length-adaptive privacy amplification in quantum key distribution[J]. Chinese Physics B, 2014, 23(9): 090310.

[6] Tan Y G, Liu Q. Measurement-device-independent quantum key distribution with two-way local operations and classical communications[J]. Chinese Physics Letters, 2016, 33(9): 090303.

[7] Li Mo, Zhang Chunmei, Yin Zhenqiang, *et al*. An overview on the post-processing procedure in quantum key distribution[J]. Journal of Cryptologic Research, 2015, 2(2): 113-121.
李　默, 张春梅, 银振强, 等. 量子密钥分配处理概述[J]. 密码学报, 2015, 2(2): 113-121.

[8] Yuen H P. Security issues associated with error correction and privacy amplification in quantum key distribution[EB/OL]. (2014-11-10)[2016-08-14]. https://arxiv.org/pdf/1411.2310.pdf.

[9] Carter J L, Wegman M N. Universal classes of hash functions[J]. Journal of Computer & System Sciences, 1979, 18(2): 143-154.

[10] Hayashi M, Tsurumaru T. More efficient privacy amplification with less random seeds via dual universal Hash function [J]. IEEE Transactions on Information Theory, 2016, 62(4): 2213-2232.

[11] Trevisan L. Extractors and pseudorandom generators[J]. Journal of the ACM, 2001, 48(4): 860-879.

[12] De A, Portmann C, Vidick T, *et al*. Trevisan's extractor in the presence of quantum side information[J]. SIAM Journal on Computing, 2012, 41(4): 915-940.

[13] Berta M, Fawzi O, Scholz V B. Quantum-proof randomness extractors via operator space theory[EB/OL]. (2014-09-11)[2016-08-14]. https: //arxiv.org/pdf/1409.3563v2.pdf.

[14] Bennett C H, Brassard G, Robert J M. Privacyamplification by public discussion[J]. SIAM Journal on Computing, 1988, 17(2): 210-229.

[15] Bennett C H, Brassard G, Crepeau C, *et al*. Generalized privacy amplification[C]. Proceedings of IEEE International Symposium on Information Theory, 1995, 41(6): 1915-1923.

[16] Miller C A, Shi Y. Robust protocolsfor securely expanding randomness and distributing keys using untrusted quantum devices[EB/OL]. (2016-07-29)[2016-08-14]. https: //arxiv.org/pdf/1402.0489v4.pdf.

[17] Krawczyk H. LFSR-based hashing and authentication[C]. CRYPTO '94 Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology, 1994, 839: 129-139.

[18] Fung C H F, Ma X, Chau H F, *et al*. Quantum key distribution with delayed privacy amplification and its application to security proof of a two-way deterministic protocol[J]. Physical Review A, 2012, 85(3): 032308.

[19] Nisan N, Wigderson A. Hardness vs randomness[J]. Journal of Computer & System Sciences, 1994, 49(2): 149-167.

[20] Renner R. Security of quantum key distribution[J]. International Journal of Quantum Information, 2008, 6(1): 1-127.

[21] Ran R, Reingold O, Vadhan S. Extracting all the randomness and reducing the error in Trevisan's extractors[J]. Journal of Computer and System Sciences, 2002, 65(1): 97-128.

[22] Mauerer W, Portmann C, Scholz V B. A modular framework for randomness extraction based on Trevisan's construction[EB/OL]. (2012-12-03)[2016-08-14]. https: //arxiv.org/pdf/1212.0520v1.pdf.

[23] Konig R T, Terhal B M. The bounded-storage model in the presence of a quantum adversary[J]. IEEE Transactions on Information Theory, 2008, 54(2): 749-762.

[24] Tomamichel M, Schaffner C, Smith A, *et al*. Leftover hashing against quantum side information[J]. IEEE Transactions on Information Theory, 2011, 57(8): 5524-5535.

[25] Ma X, Xu F, Xu H, *et al*. Postprocessing for quantum random number generators: Entropy evaluation and randomness extraction[J]. Physical Review A, 2013, 87(6): 062327.