中国科学技术大学
University of Science and Technology of China

基于FPGA的量子密钥分发系统中的身份认证方案的实现

王坚　崔珂

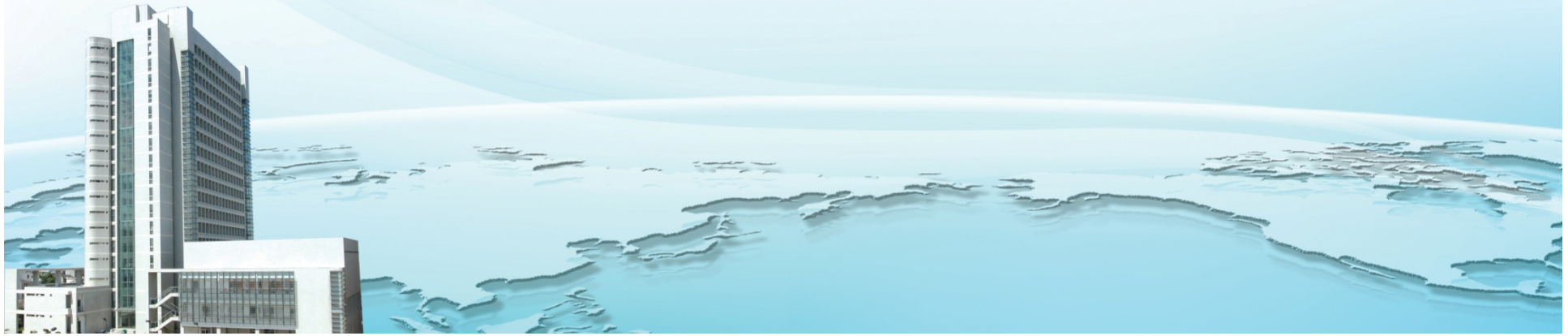
核探测与核电子学国家重点实验室

中国科学技术大学 近代物理系

报告内容

中国科学技术大学
University of Science and Technology of China

- 1.量子密钥系统和身份认证目的，功能
- 2.原理
- 3.硬件算法流程



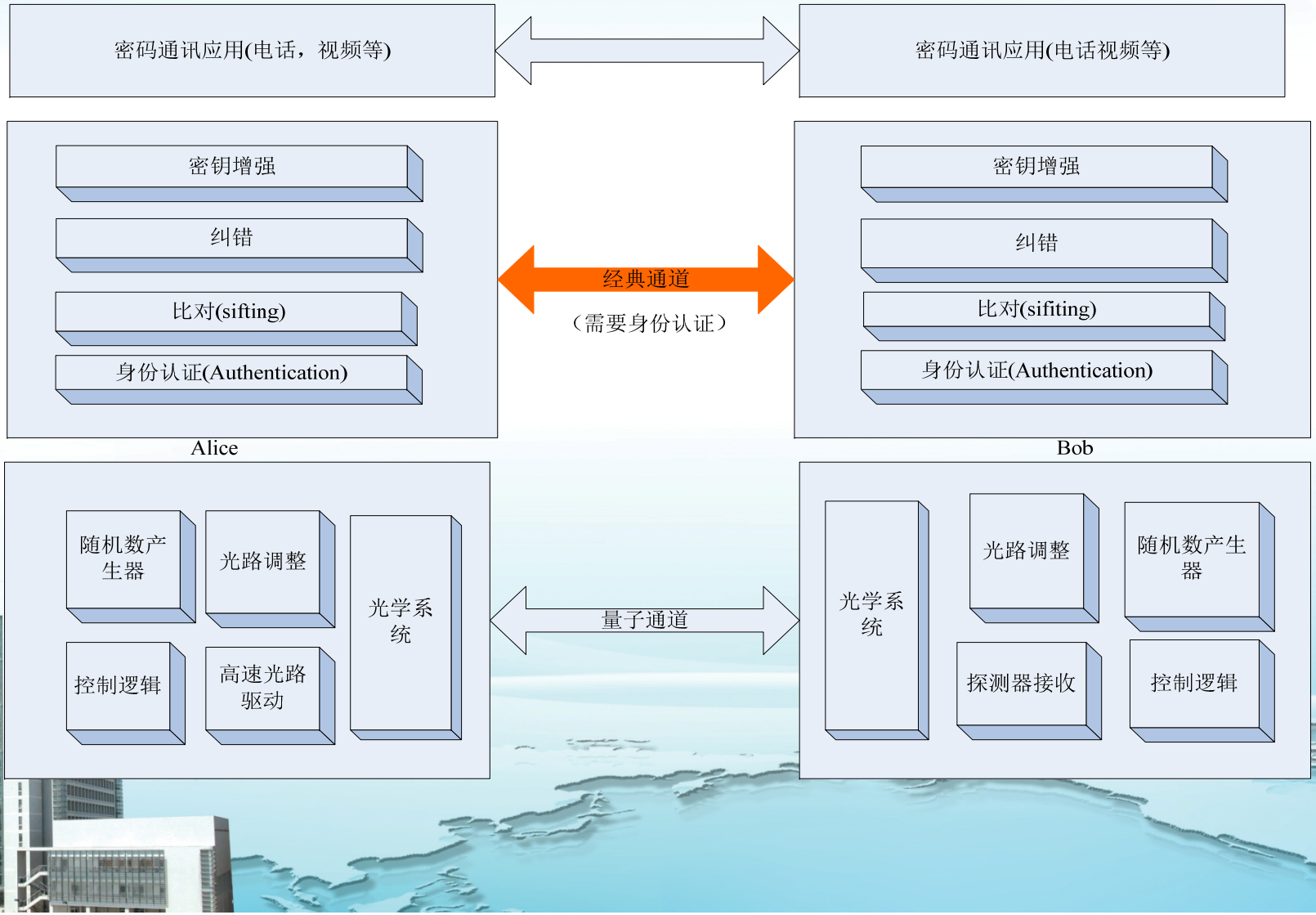
基于decoy和BB84协议的量子密钥系统

中国科学技术大学
University of Science and Technology of China

- 量子密钥分发系统（Quantum key distribution--QKD）是近二十多年来发展迅速的安全通讯技术,它是由量子物理中的不可克隆定理保证安全性，只要量子物理的基本假设不被推翻，它就是绝对安全的。
- 最早出现也是应用最广泛的是BB84以及加入decoy协议的改进BB84方案，与电子学相关的后处理过程括以下三个基本步骤：基矢比对，纠错和隐私放大。

量子密钥系统

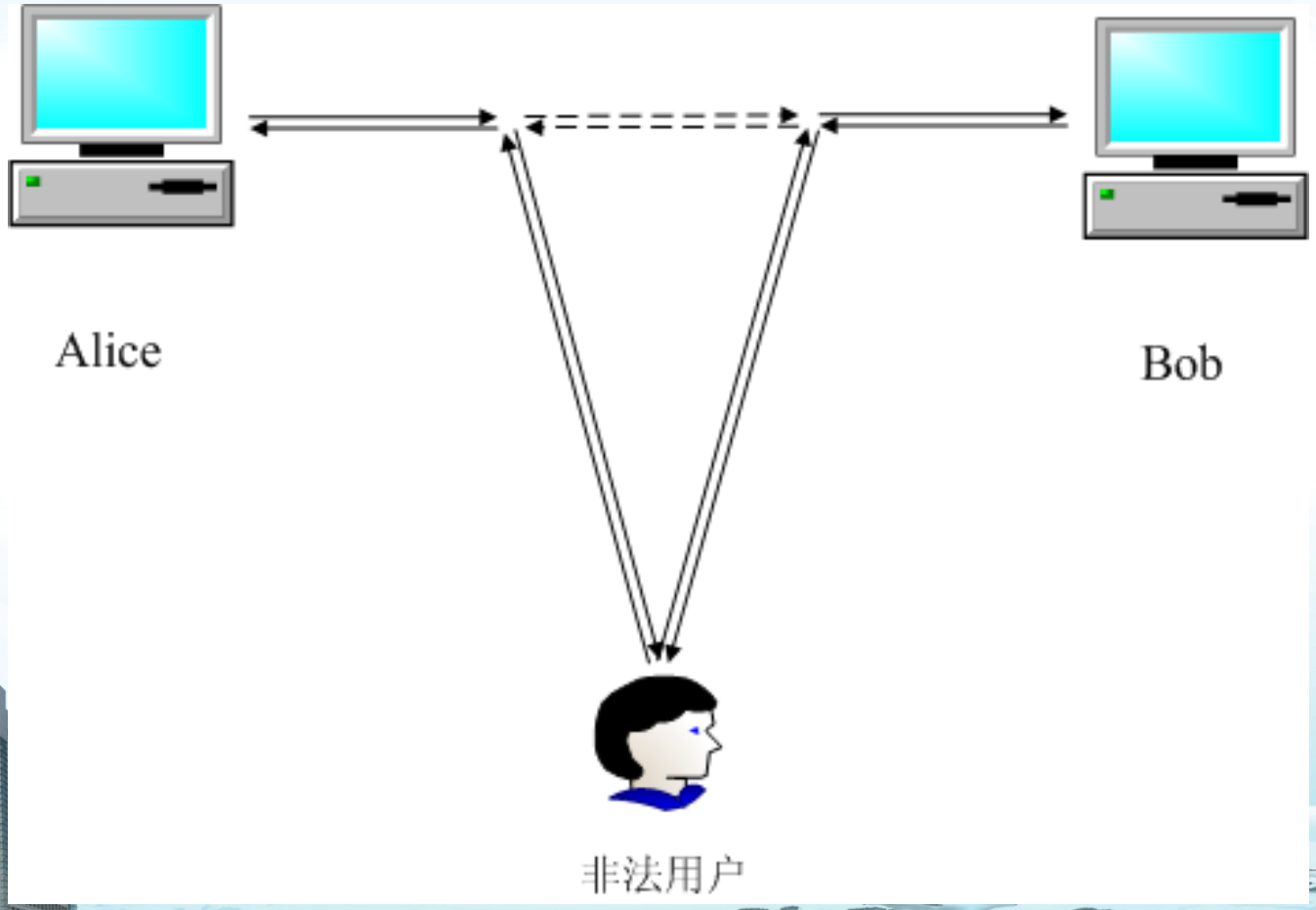
中国科学技术大学
University of Science and Technology of China



身份认证目的，功能

- 目的：授权量子通讯系统中的经典信息通路，认证通讯过程中基矢比对过程需要交互的信息，防止中间人攻击。
- 所谓中间人攻击：就是指攻击者与通讯的两端分别建立独立的联系，并交换其所收到的数据，使通讯的两端认为他们正在通过一个私密的连接与对方直接对话，但事实上整个会话都被攻击者完全控制。

身份认证目的，功能



身份认证目的，功能

中国科学技术大学
University of Science and Technology of China

功能：Alice和Bob对基矢比对过程中经典信道中所传输的数据按照约定算法进行哈希处理得到一串码字，利用双方共享的一段加密密钥对者串码字加密完后得到认证码（tag）。比较双方的认证码是否一致，从而得到认证结果。

身份认证原理---Teoplitz矩阵

- 哈希函数族采用Teoplitz矩阵，它简单易于构造。
- Teopliz矩阵具如下有性质：假设$a_{i,j}$和$b_{m,n}$是Teopliz矩阵中的任意两个元素，如果i-j=m-n；那么$a_{i,j}=b_{m,n}$。简单的说，后面一列的数据是前面一列数据向下（或向上）移动一个bit，再在该列最上面（或最下面）补充上一个新的bit。这样确定一个Teopliz矩阵需要n+m-1 bits，其中n是Teopliz矩阵行数，m是Teopliz矩阵的列数。

Teoplitz矩阵

中国科学技术大学
University of Science and Technology of China

$$h = \begin{bmatrix} s_{1,1} & s_{2,1} & \cdots & s_{m,1} \\ s_{1,2} & s_{1,1} & \cdots & s_{m-1,1} \\ \vdots & \vdots & \cdots & \vdots \\ s_{1,n} & s_{1,n-1} & \cdots & s_{m-1,n-1} \end{bmatrix}$$

身份认证原理---基于LFSR的Teoplitz矩阵

中国科学技术大学
University of Science and Technology of China

基于LFSR的Teopliz矩阵对上面的bits数目加以减少，第一列数据仍然需要n bits，但是第一行的数据m-1 bit不需要了，这些数据由前面一列的若干行的数据异或结果获得，异或数据的位置由对应长度LFSR多项式规定的bits位置确定。这样Teopliz矩阵长度需求量减少到n+n bits，其中n bit确定LFSR多项式，n bit确定Teopliz第一列数据。一般来说n<<m，所以这种方案可以节约大量存储资源。

身份认证原理

中国科学技术大学
University of Science and Technology of China

- 认证的时候，用Teopliz矩阵乘以长度为m的信息数据得到长度为n的认证数据n1，然后取一个长度也为n的随机序列r，得到最终的认证码n2=n1^r。
- 认证需要对基矢比对过程中每次传递的信息组加以认证，认证实现过程中的两种方法：
- ①对每个信息组更新Teoplitz矩阵的第一列数据
- ②对每个信息组更新r；我们采用此种方案

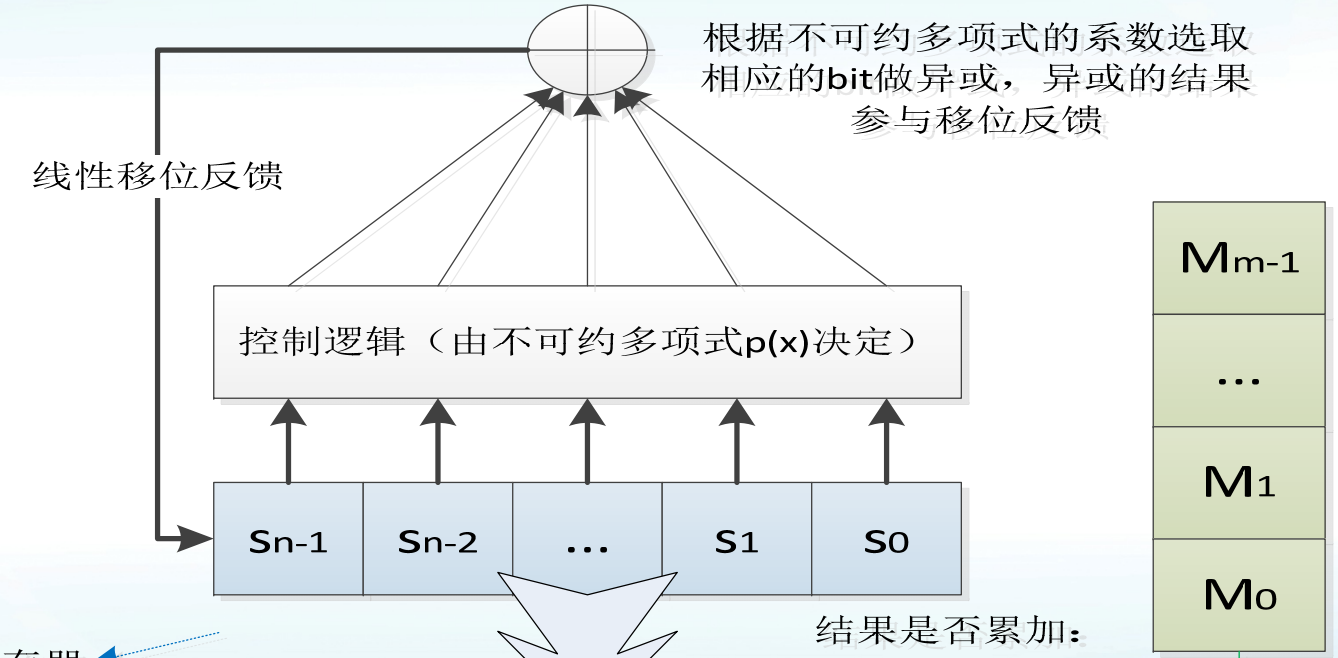
对于长度m的信息 $\mathrm{M} = (M_0 \quad M_1 \quad \cdots \quad M_{m-1})$

用h(M)表示矩阵相乘的结果。矢量乘以一个矩阵的结果可以写成如下表达式：

$$\mathrm{h(M)} = \oplus_{j=0}^{m-1} \{M_j \cdot (s_{j,1}, s_{j-1,1}, \cdots, s_{j-1,n-1})\}$$

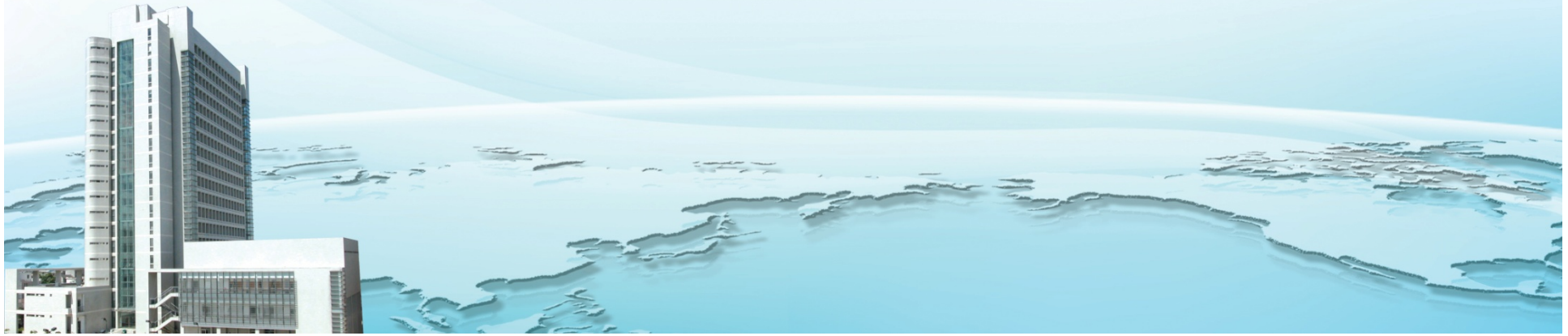
基于FPGA的算法流程

中国科学技术大学
University of Science and Technology of China



对密钥量的消耗

设认证对密钥码率的需求速度是y bits/s，基矢比对一个经典信道的信息速度是x_i bits/s，则$y=(x_1+...+x_{i)}*n/m$ bits/s。一般n固定取为256 bits或 512 bits。采用大的m值，可以降低对于密钥码率的需求。



FPGA实现

中国科学技术大学
University of Science and Technology of China

·上述算法适于硬件实现，所有操作都是模2的异或，本算法采用FPGA实现。FPGA的型号是Ateral公司的一款低端FPGA：EP3C120F780C7.

·实现后的逻辑资源消耗如下：

逻辑资源：7118/119008(6%)

存储资源：818176/3981312(20%)

资源消耗低。

中国科学技术大学
University of Science and Technology of China

感谢各位！