芯片化量子密钥分发

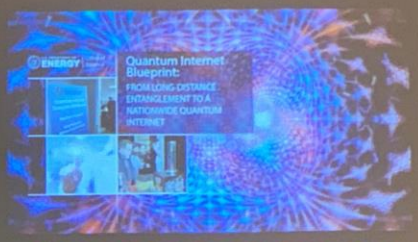
徐飞虎 (Feihu Xu)

物理学院&合肥微尺度物质科学国家研究中心

中国科学技术大学(USTC)

量子网络：激烈的国际竞争

Chen et al., Nature 589, 214 (2021)



2020年7月美国能源部计划10年内建成“国家量子互联网”

未来量子网络所面临的挑战

安全性？

⬇

现实安全性

远距离？

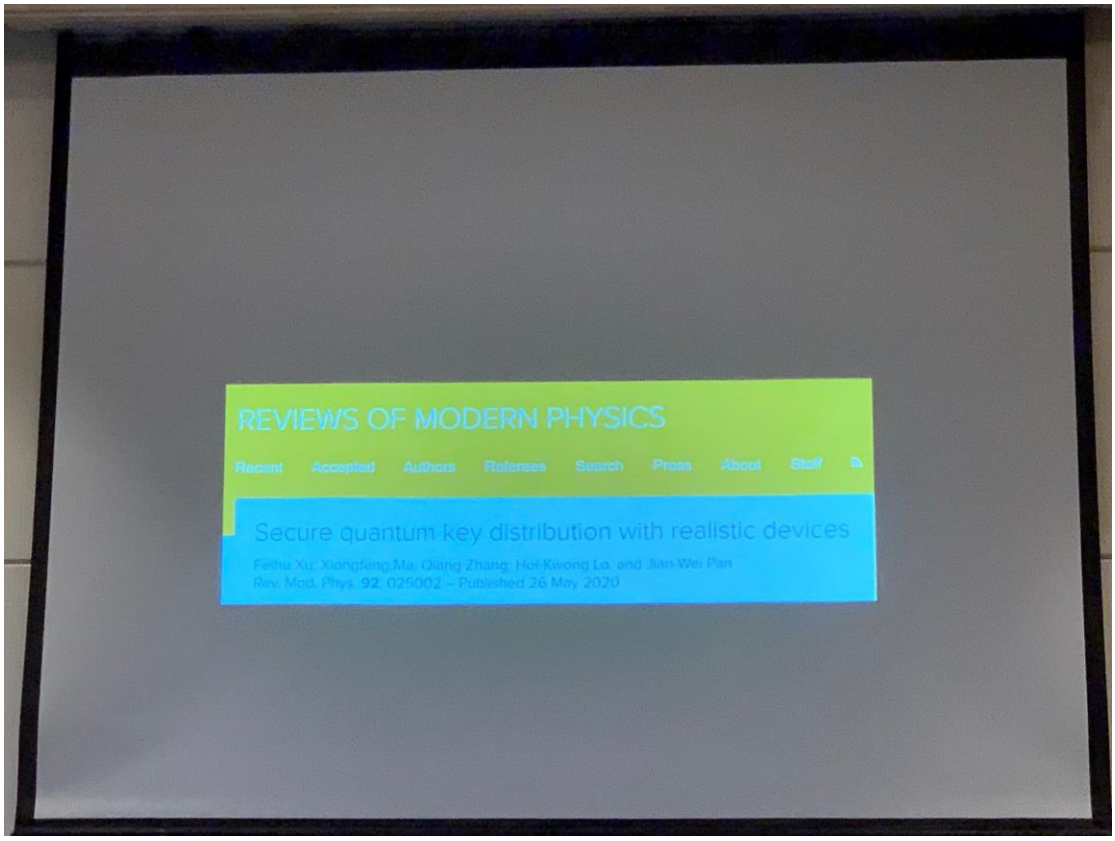
⬇

量子中继

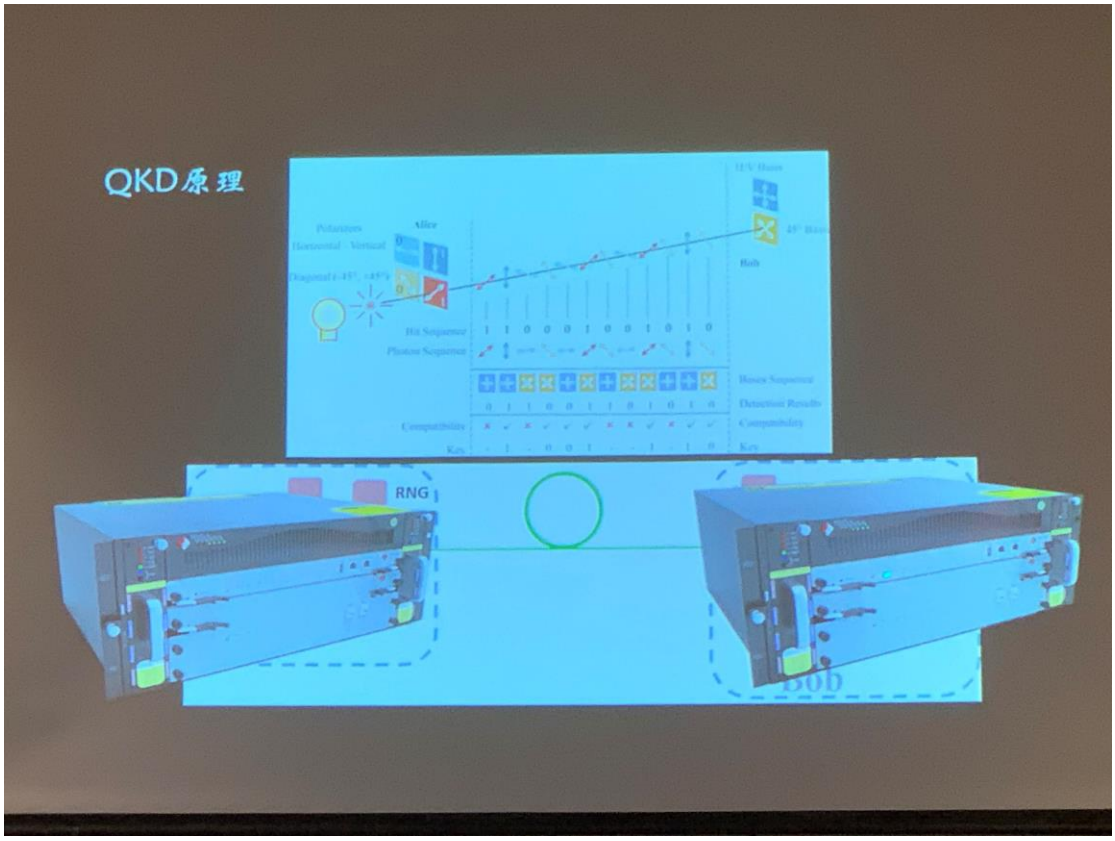
应用？

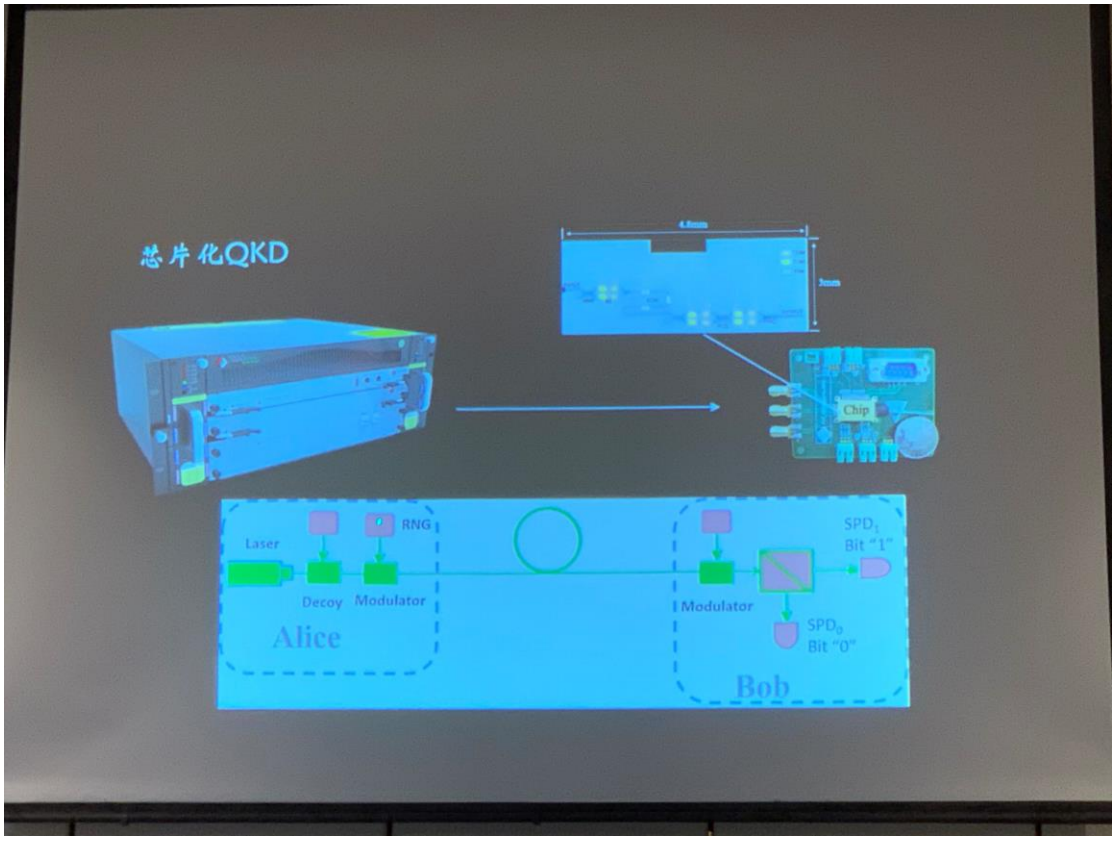
⬇

低成本、小型化


REVIEWS OF MODERN PHYSICS
Recent Accepted Authors Referees Search Press About Staff
Secure quantum key distribution with realistic devices
Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan
Rev. Mod. Phys. 92, 025002 – Published 26 May 2020

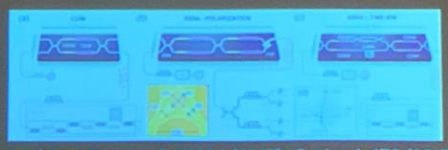

QKD原理
Laser
RNG
Decoy
Modulator
Alice
Modulator
SPD1
Bit "1"
SPD0
Bit "0"
Bob


QKD原理
Alice
Bob
RNG

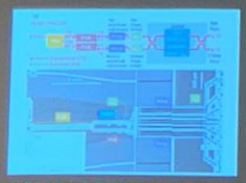

芯片化QKD
Chip
Laser
RNG
Decoy
Modulator
Alice
Modulator
SPD1
Bit "1"
SPD0
Bit "0"
Bob

芯片化QKD近期进展

Toronto: Optica 3, 1274 (2016)



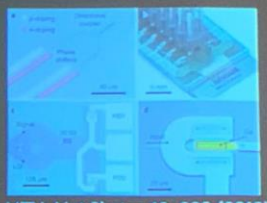
Bristol: Nat Commun 8, 13984 (2017); Optica 4, 172 (2017)



Sandia NL: OE 25, 12282 (2017)

Denmark: npj Quant Inf 3, 25 (2017)

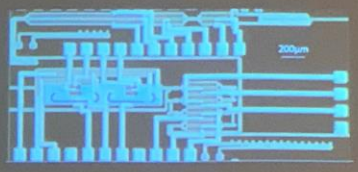
MIT: PRX 8, 021009 (2018)



NTU: Nat Photon 13, 839 (2019)
USTC: PRX 10, 031030 (2020)

举例1：硅光子芯片BB84发射端

与 Joyce Poon 组合作 (Toronto)



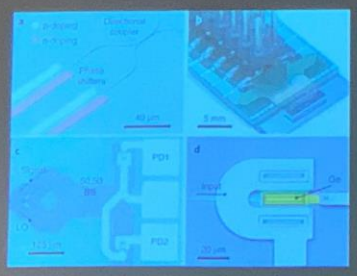
3mm x 1mm

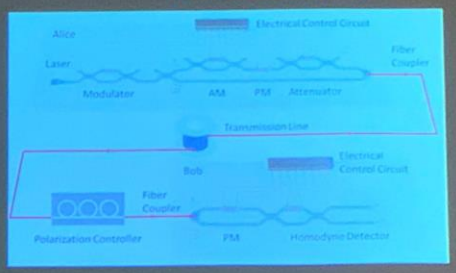
- 高性能器件
  - 环形调制器：20 dB ER，支持 GHz 调制
  - 偏振调制器：>30 dB ER，0.9 dB 功率抖动
- BB84演示
  - QBER: 5.4%；安全密钥率：0.95 kbps

Ma et al., Optica 3, 1274 (2016)

举例2：硅光子芯片连续变量QKD

与 Ai-Qun Liu组合作 (NTU)



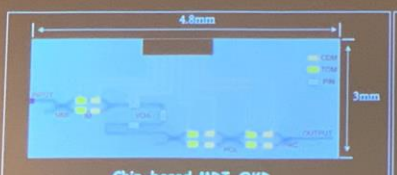


硅芯片上集成低噪声零差探测器
10MHz bandwidth, 5dB shot-noise clearance

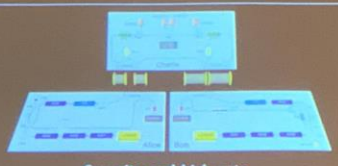
验证性实验演示CV-QKD

Zhang, ..., Xu*, Liu* Nature Photon. 13, 839 (2019)

Chip-based MDI-QKD

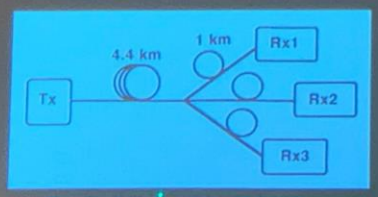


Chip-based MDI-QKD
[Wei, Xu* et al., PRX 10, 031030 (2020)]

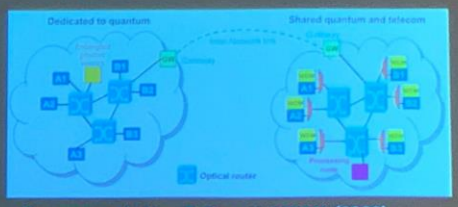


Security and high rate
[Li, Xu* et al., PRAppl. 15, 034081 (2021); submitted]

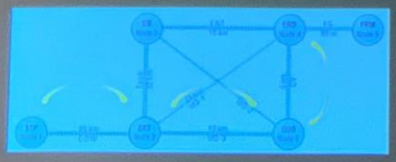
量子通信城域网：下行传输 + 可信中继



Townsend, Nature 385, 47 (1997)



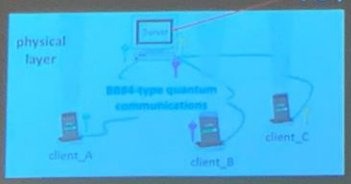
Chapuran et al., New J. Phys. 11, 105001 (2009)



- Elliott, arXiv: quant-ph/0503058 (2005) — USA
- Peev et al., New J. Phys. 11, 075001 (2009) — Europe
- Chen et al., Opt. Express 18, 27217 (2010) — China
  Wang et al. Opt. Lett. 35, 2454 (2010)
  Chen et al., Nature 589, 214 (2021)
- Sasaki et al., Opt. Express 19, 10387 (2011) — Japan

量子接入网

可信中继



Hughes et al., arXiv:1305.0305 (2013)

可信中继

Frohlich et al., Nature 501, 69 (2013)

QKD现实安全性

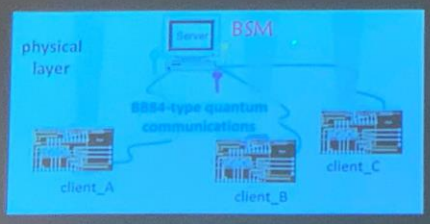
解决方案：Measurement-device-independent (MDI) QKD，根本上免除任何探测端攻击[Lo, Curty, Qi, PRL 108, 130503 (2012)]

QKD现实安全性

解决方案：Measurement-device-independent (MDI) QKD，根本上免除任何探测端攻击[Lo, Curty, Qi, PRL 108, 130503 (2012)]

基于不可信中继的量子网络组网方案

芯片化、测量设备无关(MDI)量子接入网

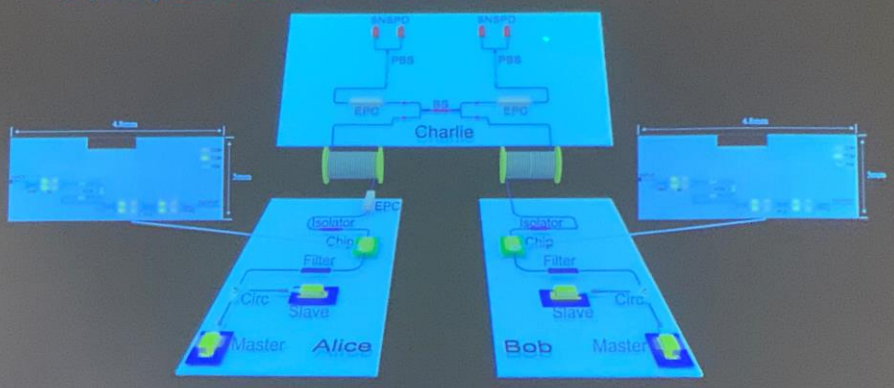


Chip-based MDI-QKD Network

- 高安全性：不可信中继
- 低成本
- 芯片：仅发射端，免受损耗影响
- 可扩展、省资源

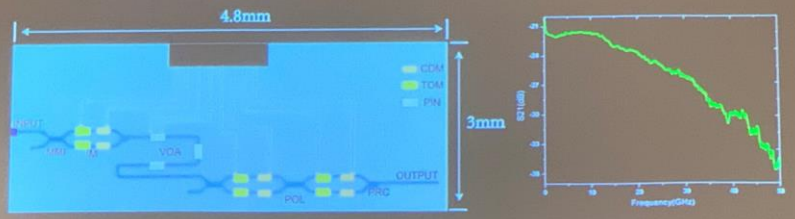
Xu et al., Nat. Photon. 9, 772 (2015)

芯片化高速MDI-QKD - 1.25 GHz



Wei, Xu* et al., PRX 10, 031030 (2020)

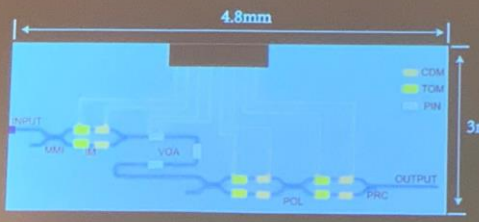
高速硅基集成调制芯片

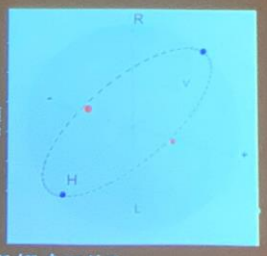


- Carrier depletion modulator (CDM) 和 MZI 结构的偏振/强度调制器
- CDM 的带宽可以达到~21 GHz

Wei, Xu* et al., PRX 10, 031030 (2020)

高速硅基集成调制芯片

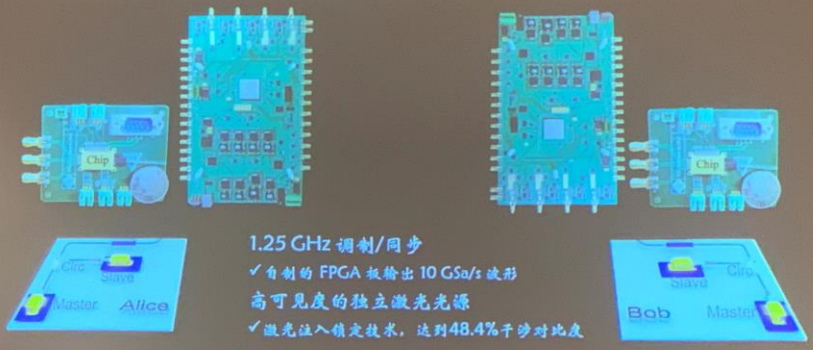




- Carrier depletion modulator (CDM) 和 MZI 结构的偏振/强度调制器
- CDM 的带宽可以达到~21 GHz
- 偏振态对比度达到~26 dB

Wei, Xu* et al., PRX 10, 031030 (2020)

GHz MDI-QKD的主要技术挑战



1.25 GHz 调制/同步

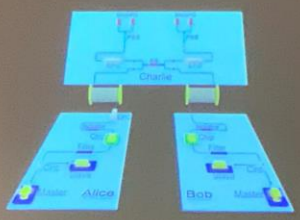
✓自制的 FPGA 板输出 10 GSa/s 波形

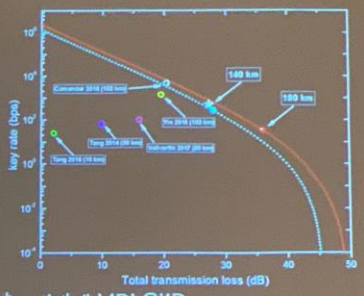
高可见度的独立激光光源

✓激光注入锁定技术，达到48.4%干涉对比度

Wei, Xu* et al., PRX 10, 031030 (2020)

GHz MDI-QKD实验结果





- 1.25 GH、随机调制诱骗态/编码态、芯片化MDI-QKD
- 硅基芯片集成了所有发射端的编码器件
- 高安全码率: 6172 (31) bits/s @ 100-km (180-km) 光纤

Wei, Xu* et al., PRX 10, 031030 (2020)

量子密码的现实安全性 Xu et al., RMP 92, 025002 (2020)

现实安全 = 理论安全 & 系统模型

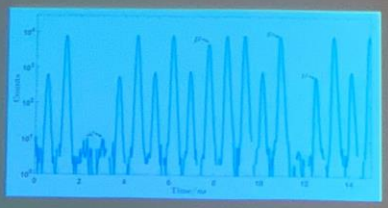
"量子攻击" 解决方案

- Side channels in high-speed QKD?
- Side channels in chip-based QKD?

Pattern effect on modulation

Pattern	average intensity of second pulse	deviation from $s \to s$
$s \to s$	1.000	-
$\mu \to s$	1.002	0.24%
$v \to s$	1.003	0.32%
$0 \to s$	1.003	0.27%
$s \to \mu$	0.617	-
$\mu \to \mu$	0.626	1.51%
$v \to \mu$	0.610	-1.08%
$0 \to \mu$	0.632	2.44%
$s \to v$	0.029	-
$\mu \to v$	0.027	-5.57%
$v \to v$	0.025	-11.95%
$0 \to v$	0.027	-5.90%

Intensity deviation is less than 12%

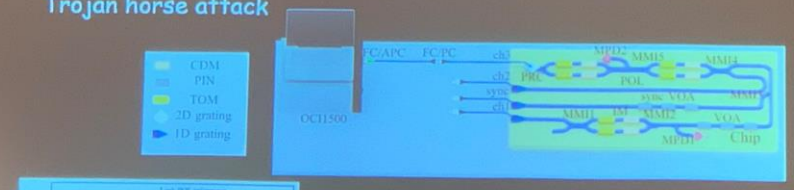


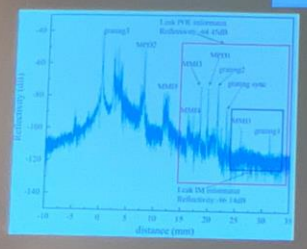
Pattern sifting + alternate key distillation

IID assumption restored

Yoshino et al., npj Quant. Inf. 4, 8 (2018)

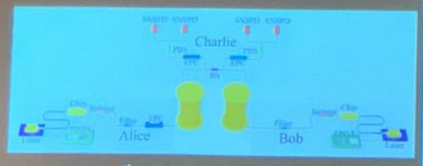
Trojan horse attack



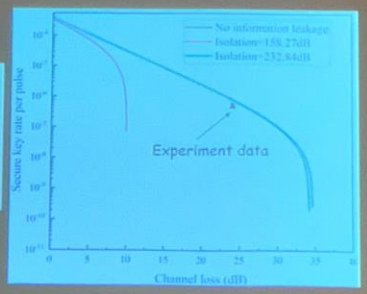


- Total reflectivity that can leak POL and IM modulation is -64.5 dB and -86.1 dB
- Lower reflectivity than fiber-based devices
- Smaller time interval between components

Chip-based MDI-QKD against THA

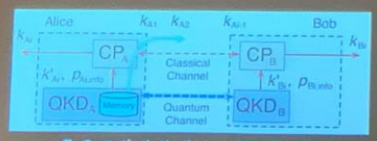


单激光器MDI-QKD

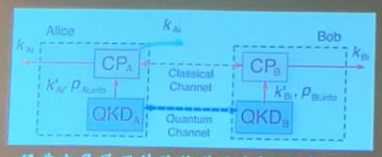


- It requires about 230 dB isolation
- MDI-QKD requires higher isolation than BB84

隐信道攻击

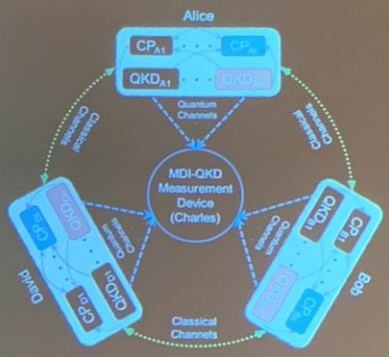


量子器件隐信道攻击(DI-QKD)



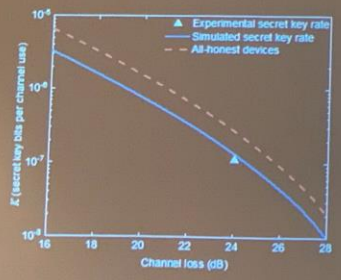
经典电子学器件隐信道攻击(经典密码)

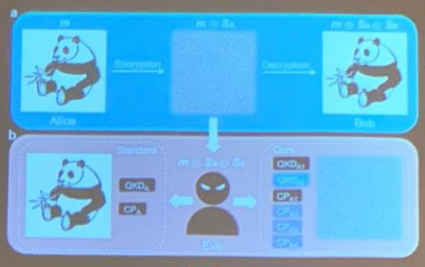
解决方案：冗余设备+多方安全计算



Curty, Lo, npj Quant. Inf. (2019)

实验演示抵制隐信道攻击

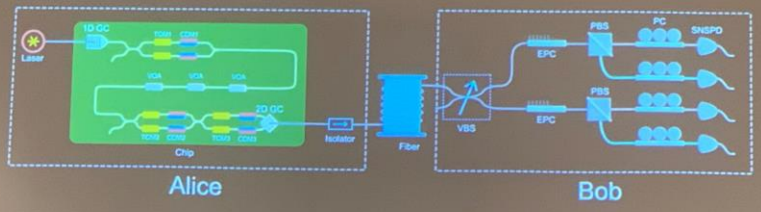




冗余设备
+
多方安全计算协议

Li, Xu* et al., PRAppl. 15, 034081 (2021)

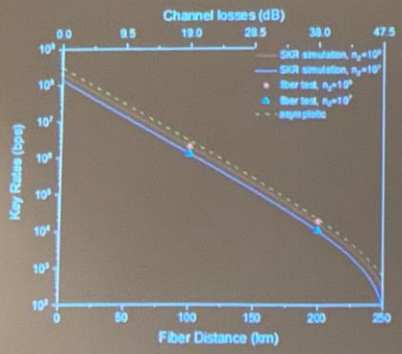
High-rate chip-based QKD



集成化：硅基发送端芯片
高速率：2.5 GHz
低误码率：0.49%
更优的BB84协议：四态、两强度

Li, Xu[a] et al., submitted (2021)

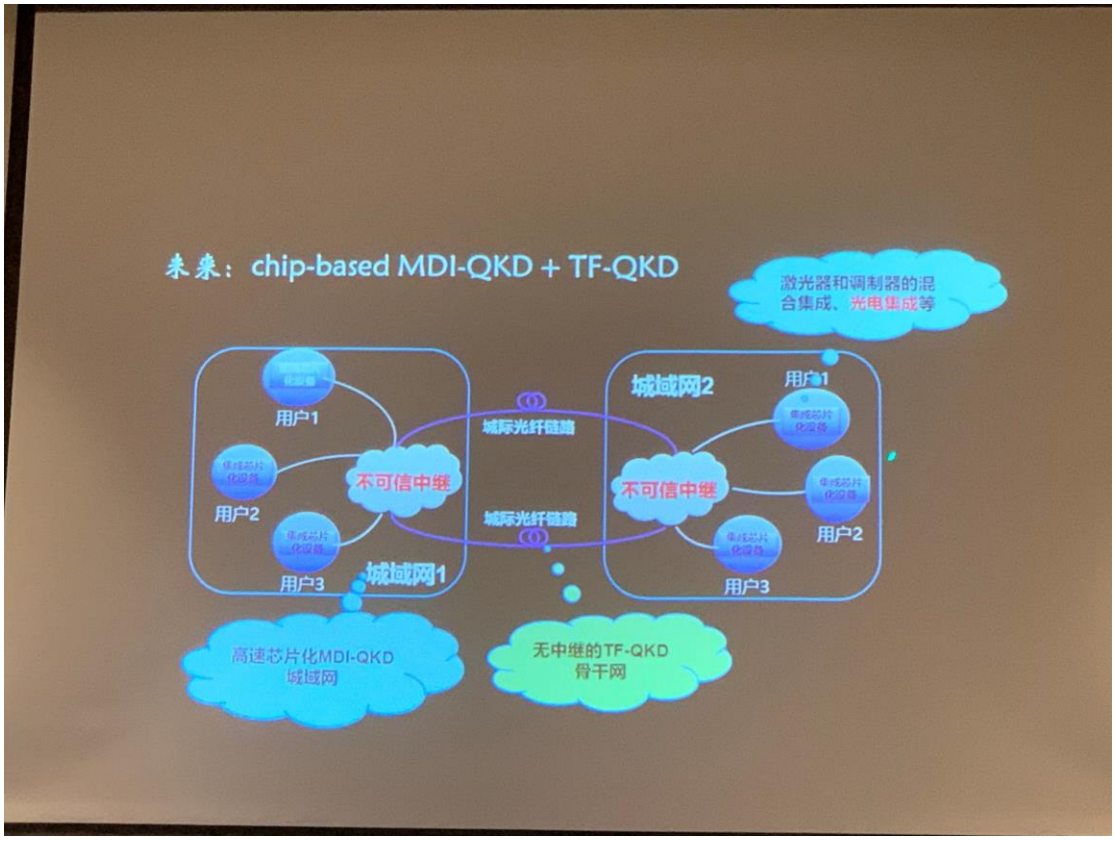
High-rate chip-based QKD

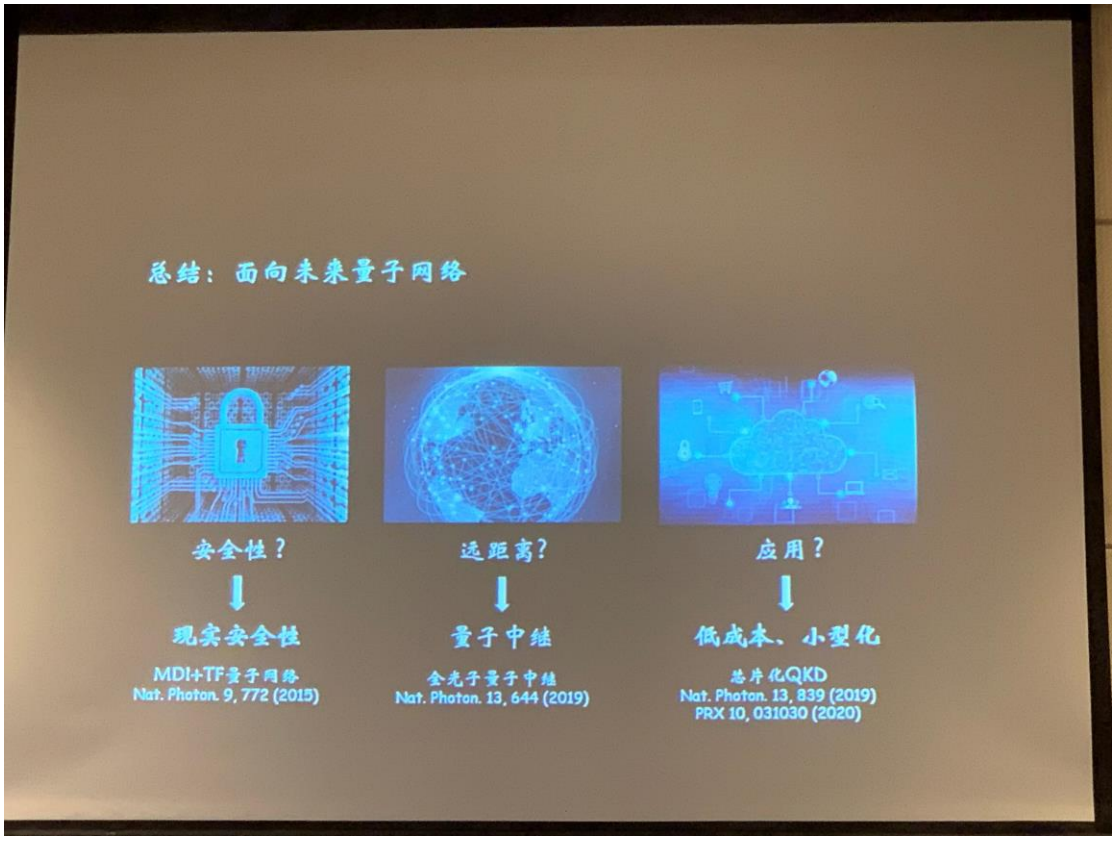


文献	协议	时钟频率	探测器	误码率	码率	码率(归一化到10 dB, Mbps)
Lucamarini et al. 2013	BB84	1 GHz	InGaAs APD(净20.5%)	4%	1.09 Mbps @50 km	1.09
Sibson et al. 2017	BB84	1 GHz	SNSPD(净40%)	1%	329 kbps @20 km	0.08
Bunandar et al. 2018	BB84	625 MHz	SNSPD(净>85%)	2%	1.039 Mbps @ 9.2 dB	0.86
Grunenfelder et al. 2020	BB84	5 GHz	SNSPD(净80%)	1.93%	392.7 kps @101 km	4.08
Islam et al. 2017	High dimension	2.5 GHz	SNSPD(净>70%)	4%	7.71 Mbps @10 dB	7.71
This work	BB84	2.5 GHz	SNSPD(净36%)	0.499%	2.4 Mbps @101 km	23.22

已报道实验中最高码率：2.4 Mbps@100km

Li, Xu[a] et al., submitted (2021)


未来：chip-based MDI-QKD + TF-QKD
激光器和调制器的混合集成、光电集成等
用户1
用户2
用户3
不可信中继
城域网1
城际光纤链路
城际光纤链路
城域网2
用户1
不可信中继
用户2
用户3
高速芯片化MDI-QKD城域网
无中继的TF-QKD骨干网


总结：面向未来量子网络
安全性？
现实安全性
MDI+TF量子网络
Nat. Photon. 9, 772 (2015)
远距离？
量子中继
全光子量子中继
Nat. Photon. 13, 644 (2019)
应用？
低成本、小型化
芯片化QKD
Nat. Photon. 13, 839 (2019)
PRX 10, 031030 (2020)