

33462 47702 21927 **General Idea** 71709 14398 07404 83493 30984 2683 15990 69706 9568 S 36609 95071 3000 96211 59313 51022 $\mathcal{A}(x)$ $\mathcal{A}(x)$ ${\mathcal D}$ ${\mathcal S}$ $\mathcal{A}(x)$ 31253 62885 78154 67471 29361 01348 95335 82377 77618 83958 98888 47154 60194 61129 2132 95598 73575 8198 22715 18860 3337 74232 83644 9712 Simple source emits a signal with probability p. The signal can be blocked by a shutter A(x). 01538 29084 80640 Mixed source is a mixture of simple sources governed by probability distribution γ known to the 45303 92293 96374 adversary, which can be fully characterized, or characterized only partially 82505 08109 17202 50377 25200 6877 Photonic example is depicted on the right. Three possible assumptions on the photon source (1) 38494 62880 36901 single photon source, (2) known photon number distribution, (3) only mean number of photons μ 78861 27891 30241 94124 66288 09828 known 67652 Protocol 92341 98013 91927 82116 68952 26540 25156 07942 Below we describe our randomness generation protocol, consisting of two parts: 23723 80997 97118 data collection and post-processing. For practical purposes, the protocol is run in 30556 64337 43443 58143 04728 49614 large batches of N rounds. 10080 09350 9304 83680 92110 56229 00408 42627 89523

1. Data Collection

From a private biased distribution, pick out $Q_i \in \{\text{TEST}, \text{GEN}\}$ at random with probability (q, 1 - q).

17606 64727 45526 99396 28748 4142 28905 77076 50719 98000 **Entropy estimates for photonic setup** 7796 49342 47491 3090 38833 70250 3537 Let us consider photonic setup given in the first box, using a beam-splitter 7319 007 81347 with reflection probability π . Solutions to the optimization problems are: 0909 055 66208 3559 669 65854 5271 525 22798 45464 6956 660 60357 91731 Single Photon: 6390 650 95139 $g^{s} = 1 - (\alpha - \beta) \left(\frac{\pi}{1 - \pi}\right)$ 4458 514 79486 08122 0118 300 6668 90' 50572 43654 2394 548 77942 **Known Photon Number Distribution:** 13201 6823 629 Define *N* implicitly 2547 621 79045 7457 359 79590 $\sum_{i=1}^{n} \gamma_i (1-\pi^i) < (\alpha-\beta); \sum_{i=1}^{n} \gamma_i (1-\pi^i) \ge (\alpha-\beta)$ 00484 2312 150 52788 25604 5191 47 59293 98975 7321 098 59008 228 43703 32002 552 76018 21772 59703 Then the guessing probability becomes 47347 38383 $g^{kd} = 1 - \frac{\pi^N}{1 - \pi^N} (\alpha - \beta) + \sum_{i=N+1}^{\infty} \gamma_i \left(\frac{1 - \pi^i}{1 - \pi^N} - 1 \right)$ 91352 17312 43069 68234 63 73228 97673 182 46752 04629 65822 545 61648 Mean Photon Number Known: 3837 094 26908 5402 272 97044 Leads to a solution with only three non-zero frequencies for 0, N and N+1 9070 503 71319 3319 612 93913 photons 4373 307 54710 43252 7100 226 64885 06461 26709 32754 0810 8271 7498 $g^{\mu} = 1 + (\alpha - \beta) - \left(\frac{(\alpha - \beta) + \mu(\pi^{N+1} - \pi^N)}{(N+1)(1 - \pi^N) - N(1 - \pi^{N+1})}\right)$ 7819 41744 76170 37259 80338 8213 53356 62915 20528 5200 11791 10633 7518 51636 33295 24672 17803

		13900	93401	00120
		60038	78361	33320
		90942	85359	92905
		88158	42330	77388
		22331	35448	80363
		38294	35780	56807
		39127	00994	26181
) Г	_ _	03845	10545	66396
.	2	90438	67883	55370
		44276	59669	12489
		89165	28357	26758
		82491	31686	54313
		16891	29691	10920
	4	23699	10724	40133
	402	20700	12194	58224
	85653	94349	68985	00900
1318	74795	25571	19490	14349
7610	60125	01720	04042	22175
1305	89749	59585	54739	41278
12	33162	94329	02004	82345
		70219	12138	88931
(184	95615	26199	93320
	1	98574	11094	75944
Tł	/	81620	77149	06787
	/	37978	28407	49949
CO		86942	02535	60035
		17399	17303	62500
		68515	68670	55800
Ext		03064	51359	92994
		49434	92148	00170
•		12694	93993	54145
		85828	69909	09361
		28756	39344	00038
•		03007	74422	89980
C		28561	50547	58096
S_N 1)		35134	73832	68934
1)		63397	03843	08373
т,		73916	43118	72231
•		59383	63109	46886
•		75208	41499	55308
-		10044		1

17170 72049 13944

87389 60654

98234 58302

76308

65485 98353 91460

27101 38506 00429

69894 04952 82104

00315 00149 57326

66128 93481 13968

22555 40610

01012 28980

69394 42848

- II. If $Q_i = \text{TEST}$: Pick out $x_i \in \{0,1\}$ at random with probability $(\frac{1}{2}, \frac{1}{2})$, which will determine whether to leave the shutter open (x = 0) or *closed* (x = 1). The outcome frequencies are used to update S_{exp} .
- III. If $Q_i = \text{GEN}$: Use $x_i = 0$ for the round, record the output y_i .

2. Post-Processing

- Estimate the min-entropy $H_{\min}(Y)$ of Y based on the test statistics S_e and desired assumptions.
- II. Use a universal hash-function to obtain a string Z of length $H_{\min}(Y)$ up to ϵ error.

88584 35355 36111

Optimization problems

The main goal is to upper bound the guessing probability g^* of an adversary correlated with untrusted the measurement devices.

31327 54526 71258 26743 28593

Extremal Deterministic strategies of detectors

- In simple source scenario strategies are: "Never Click", "Always Click", "Click if it detects signal".
- Correspondingly, they would produce the following statistics:

 $S_N = (0,0); S_Y = (1,1); S_H = (p,0);$ where $S \coloneqq (p(\text{Click}|x = 0), p(\text{Click}|x = 0))$ 1))

- Observed statistics are then $S_e = \lambda_N S_N + \lambda_Y S_Y + \lambda_H S_H$.
- Optimization can be phrased:

8807 27722 **Experiment and results**

2460 34197 3695 5500 7783 777

1209 49570 92150

6376 98147

5299 403

1109 933

2366 410

4731 067

3383 822

65375 641

69357 222

18872 093

76384 117

61937

93 22875 732

92025 964

85780 538

92730 463

9806 39

6533 54

5747 18

5682 148

3333 779

0052 521

4552 502

2615 653

5229 736

1233 894

1767 841

5216 362

1257 882

3611 593

1453 787

5071 508

6377 966

65895 85095 04

The source is composed of a Laser and an Optical Attenuator (OA), used to reduce the power of the input light to the order of a few photons. The shutter is composed of two Polarization Controllers (POL Control), an Electro-Optical Modulator (EOM), and a Polarizer filter. If no voltage is applied to the EOM, no light passes the filter, and when a voltage is applied there is a pi-phase shift allowing light to pass the polarizer. Finally, there is a balanced beam splitter and the detector. The expected rate is 100 kbs of raw data with telecomm frequencies.

69400

69159

73335

88340

38047

89031

95368

72007

82655

99297

45608

78523

42015

77600

90649

99041

72535

01281

55493

91406

79886

21298

95689

99849

28748

03602

49852

59842 14125

12364 22648

67614 34341

715 17929 46748

90802

74746 82372

84616 03141

71497 22731

74157 94108

88461 94816

01431 93676

77614 09325

17023 69296

46352

91943

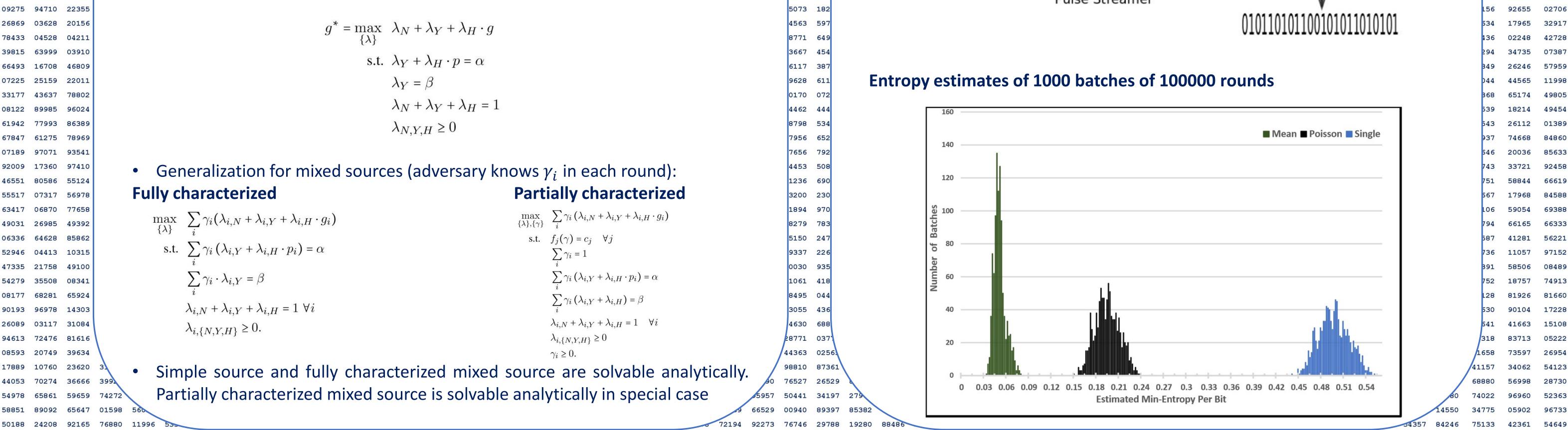
11291

27164

89842

Shutter EOM BS SNSPD ø OA Laser Diode Beam Dump Time tagger **Pulse Streamer**

The setup



87397 59315 29313 47286 87113 71922 06753 49622 99248 13083 92740 07770 17360 69012 40330 46017 55322 60873 93716 95262 49270 17992 20463 01361 21669 85449 56338 44683 64035 11558 96233 89748 07910 27364 28677 98927 71868 78678 86699