eRouška (Exposure Notification) Security, Privacy, and Impact

Tomas Rosa, Ph.D.
Cryptology and Biometrics Competence Centre of Raiffeisen BANK International in Prague

So, … Why?

To help to return to our workspace safely.

COVID-19 Mitigation Pillars

- Epidemiologists generally agree **reliable contact tracing** is among the most important safeguarding mechanism **to relief the painful lock-down measures**

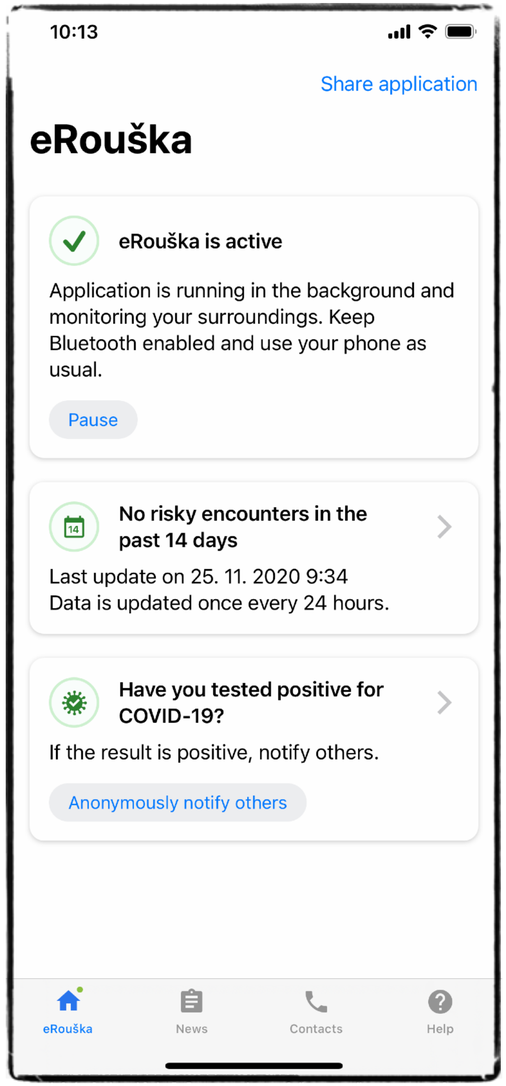
- Taking this global requirement, we can act locally as follows:

  - review the security and privacy of the eRouška application thoroughly

  - if secure enough, suggest this contact-tracing application for autonomous one-to-one risk assessments and reactions

- This can **reduce the localised reproduction number and the total viral load** in our offices significantly, as the people can be securely notified about the risk and take appropriate actions quickly by themselves

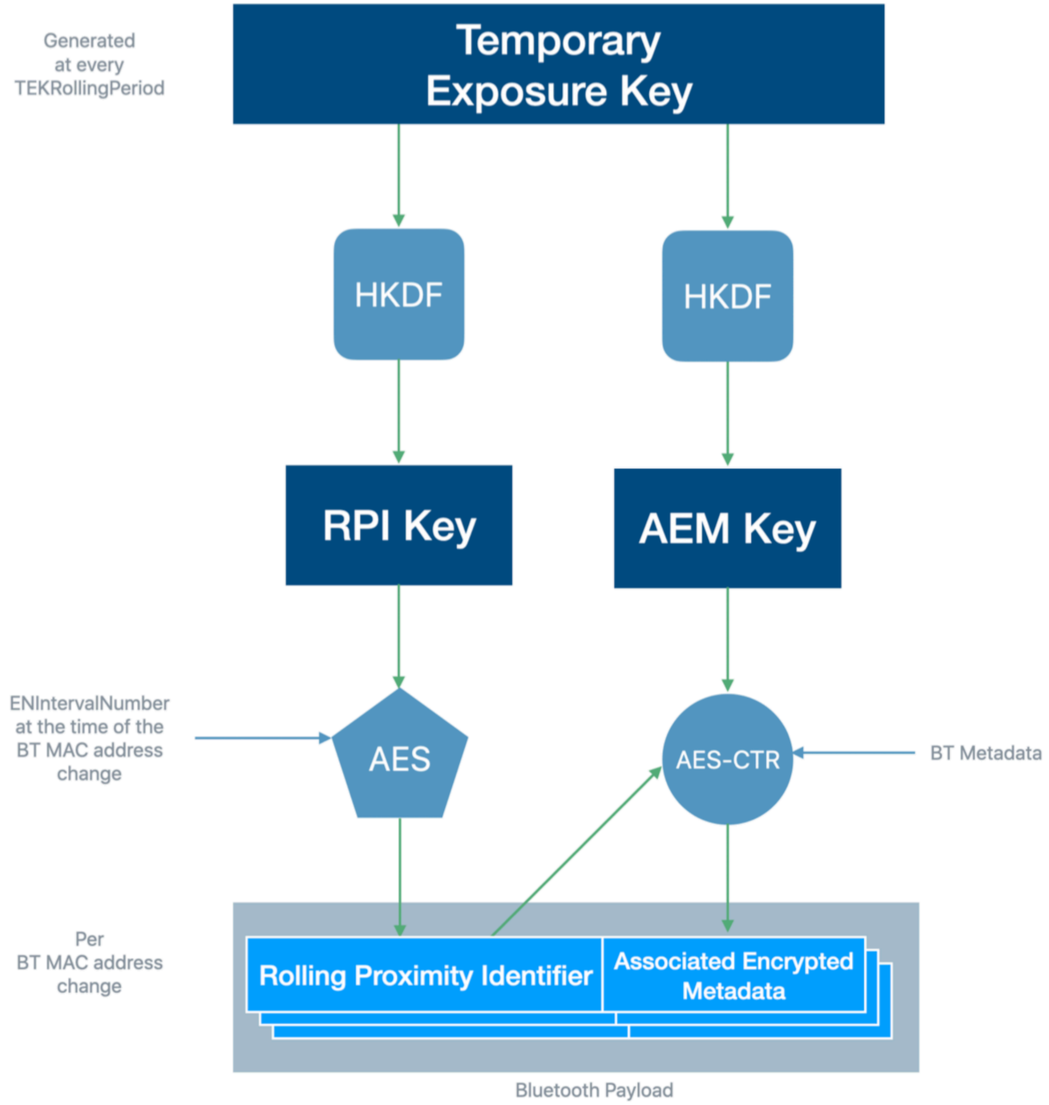
eRouška - COVID-19 Contact Tracing Application of Czech Republic



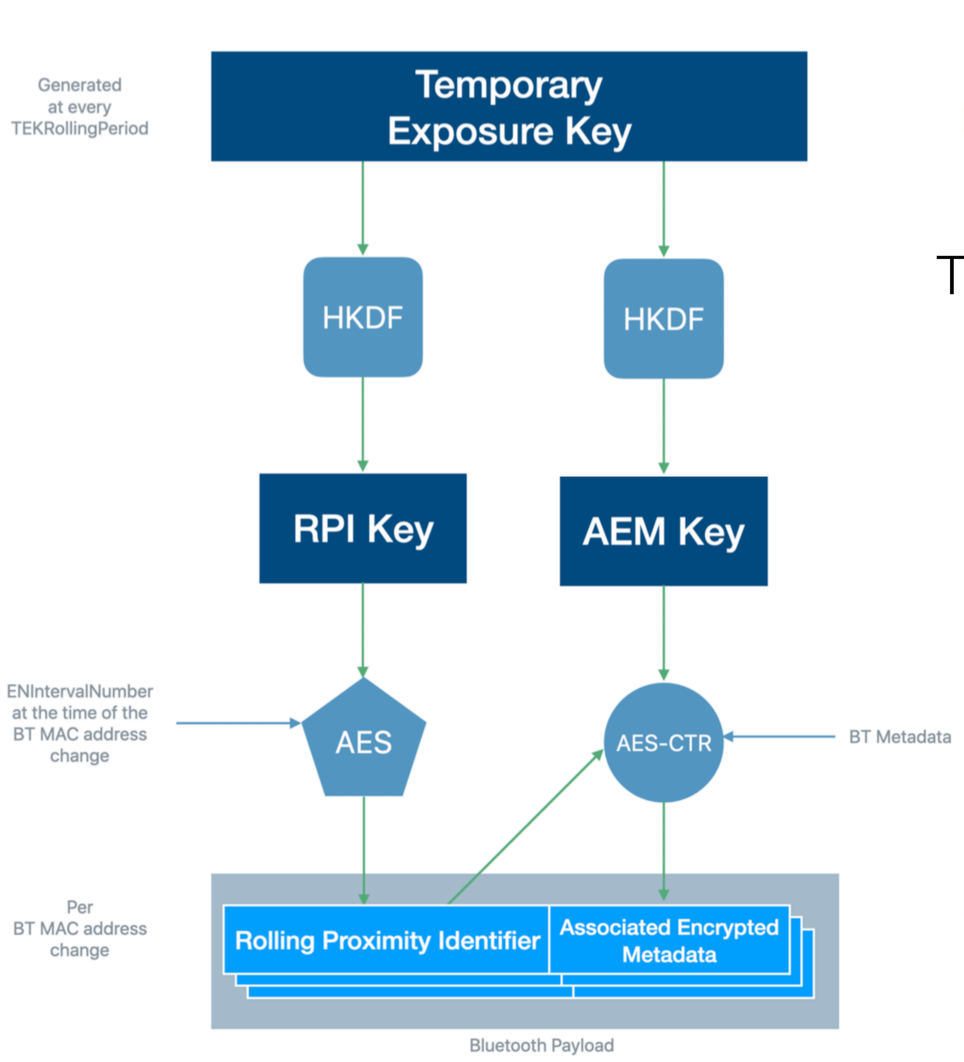
- Based on the Google-Apple Exposure Notification framework (GAEN)
- Framework is available and well-adopted worldwide
- Public health authorities of particular states can provide their own:
  - user interface application
  - risk assessment parameters
  - servers collecting keys of COVID-19 positive users

[https://erouska.cz]

Privacy Preserving Cryptographic Protocol



One-to-One Exposure Tracing Infrastructure



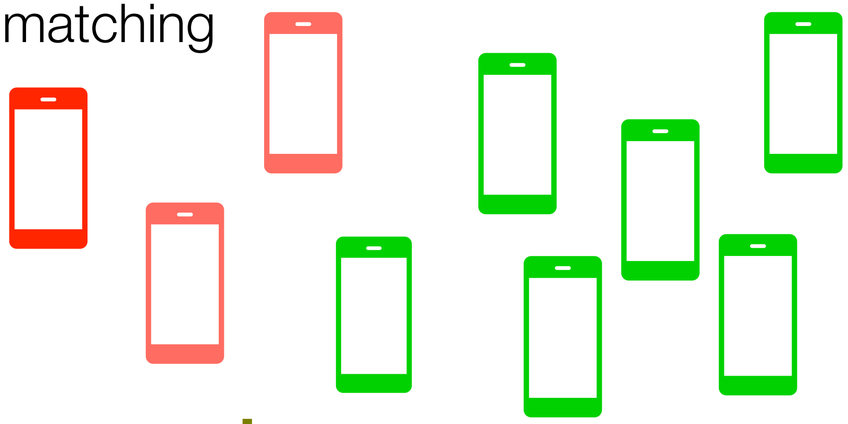
OTP-based
TCP/IP upload

Key Server
(Public Health Authority)

TCP/IP download

local matching

Bluetooth



user phones

Real Match

```
(base) macwell:cz tom$ ../../../bin/kfsp < 1605312000-1605398400…
...
7FC18B829AE9F91B0CA1870C5C253C8C 2 2673504 [2020-10-31,01:00] 144 1 -11
7FC206064BA6F5F9D666D16FF116E7E0 2 2674800 [2020-11-09,01:00] 144 1 0
7FCFB233659F5E79057F2CF5191A5D34 2 2674656 [2020-11-08,01:00] 144 1 -4
7FD5BC66FB6D59A6E16B3DEA7CE348D5 2 2674656 [2020-11-08,01:00] 144 1 -4
...
```

daily key export

```
(base) macwell:adv tom$ cat QTH-Petrovice/2020-11-09-1.adv
...
035A6EC1C5916B1B881C6ADC273C46FE -92 4
03F82E7A6A3951E0EA27200F2C8B31EB -84 1
0415DFE65EACD88769BD33B9CCC4A42D -82 25
042AF6B7C44131B721147D83BADCDA34 -83 14
...
1F324B33C004BA505A78BC8DE8FAE3B5 -82 96
1F3C10FC4025FB6166DA0A7190AC033E -83 223
1F3C963CA5B177D0B4F
...
24211A70A7969270A39
2480BE59291D66698DB
24C616A59E08DCDE9BE
24D5BD7E8CB3AC70BA2
...
```

Bluetooth scan

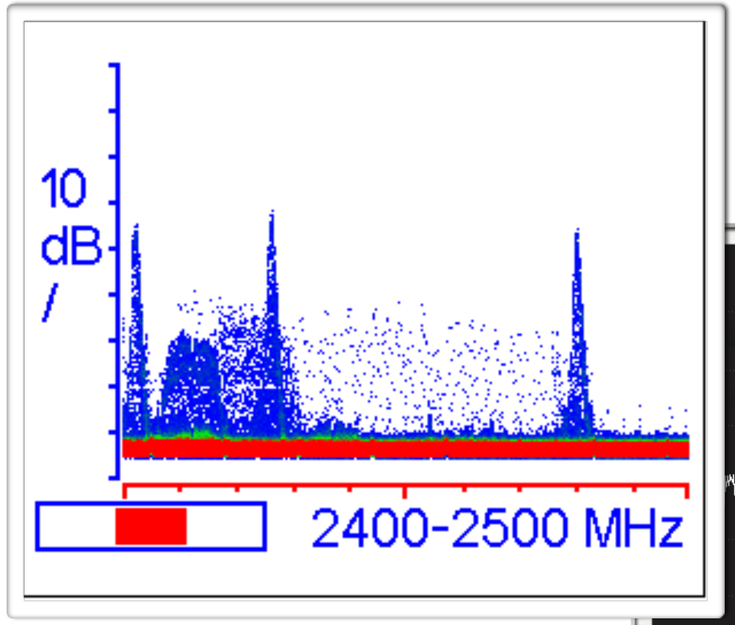
derive

compare

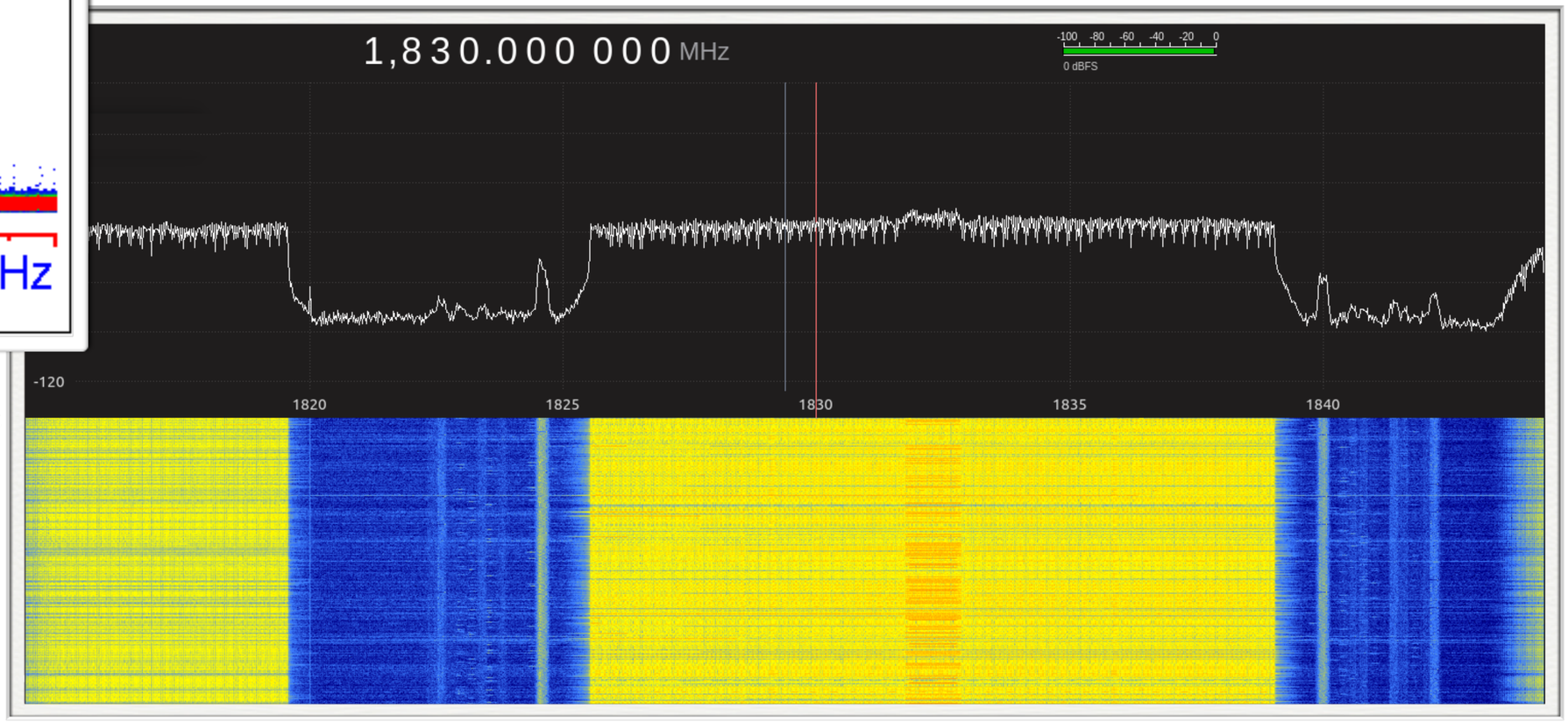
```
(base) macwell:cz tom$ rpigen 7FC206064BA6F5F9D666D16FF116E7E0 2674800 144 …
...
52278574C5AC961A255B78AFC3EA1E81 5165918E 2674809 [2020-11-09,02:30] 7FC2060…
2480BE59291D66698DBE2CA96374C0DB 56899872 2674810 [2020-11-09,02:40] 7FC2060…
076F3AEDFEA4359A6A5326111ABC0EC4 4C324595 2674811 [2020-11-09,02:50] 7FC2060…
1F3C10FC4025FB6166DA0A7190AC033E 9FDA7FD3 2674812 [2020-11-09,03:00] 7FC2060…
ABF3B6D6C75C7A9A98BE8760FE2A7B85 BF9D4341 2674813 [2020-11-09,03:10] 7FC2060…
03F82E7A6A3951E0EA27200F2C8B31EB 5B418588 2674814 [2020-11-09,03:20] 7FC2060…
764AEDB26481CECF7FB506AD04E71B8E FC8F9D2D 2674815 [2020-11-09,03:30] 7FC2060…
...
```

rolling proximity identifiers

eRouška Signal vs LTE Radio Activity



advertisement channels peaks at
2402 MHz, 2426 MHz, and 2480 MHz

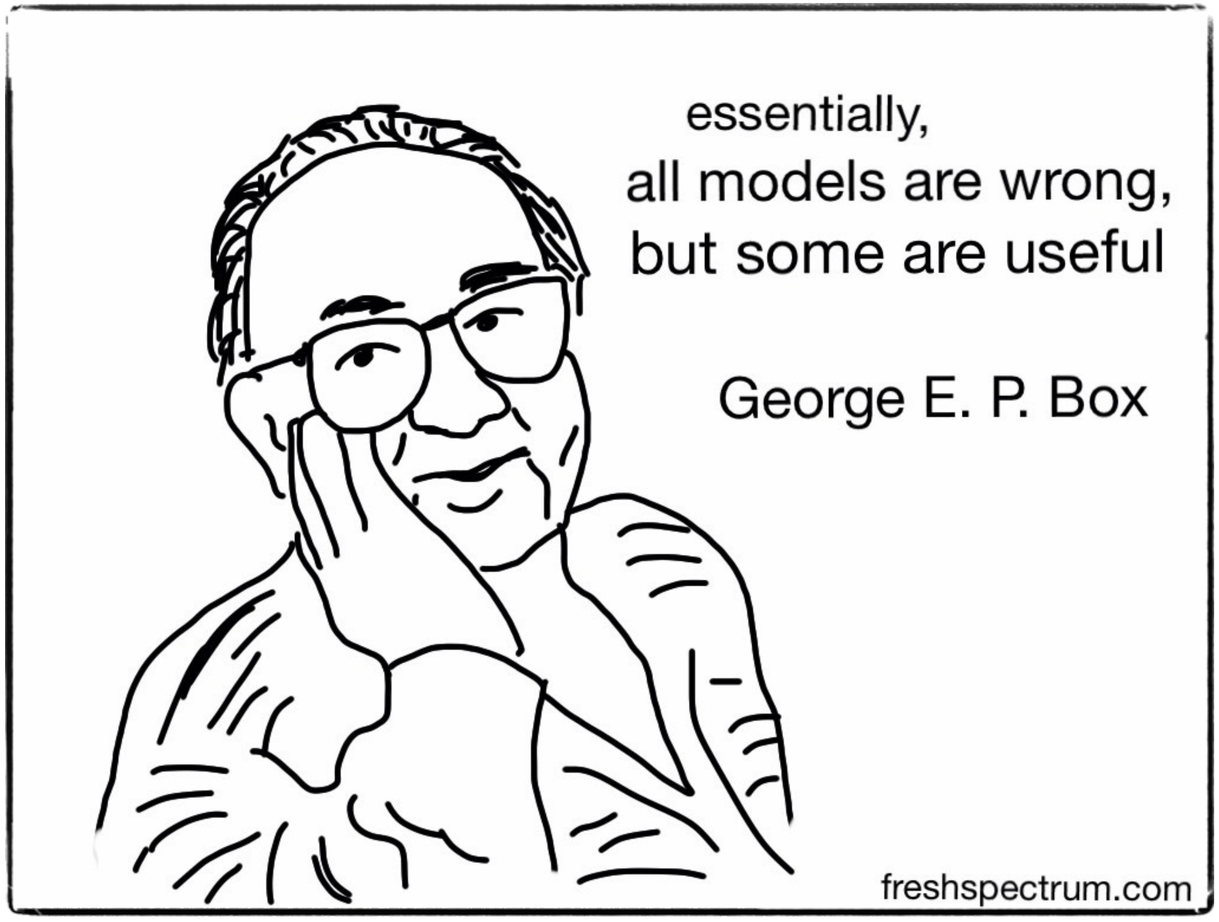


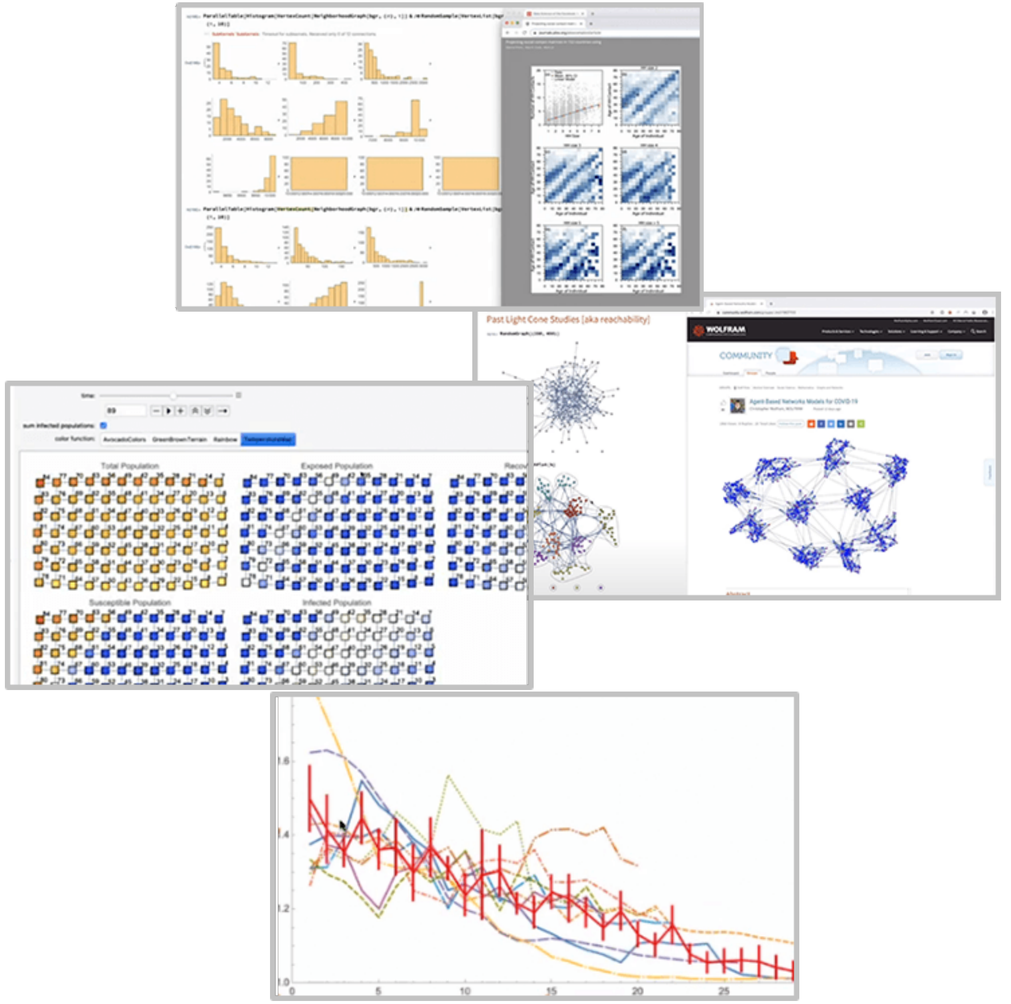
15 MHz broadband bandwidth of 4G

Résumé

If we are not worried about using the mobile phone in itself (for calls, SMS, internet, etc.), then using eRouška will not bring us any new risk, whatsoever.

Have You Said “Modelling”?



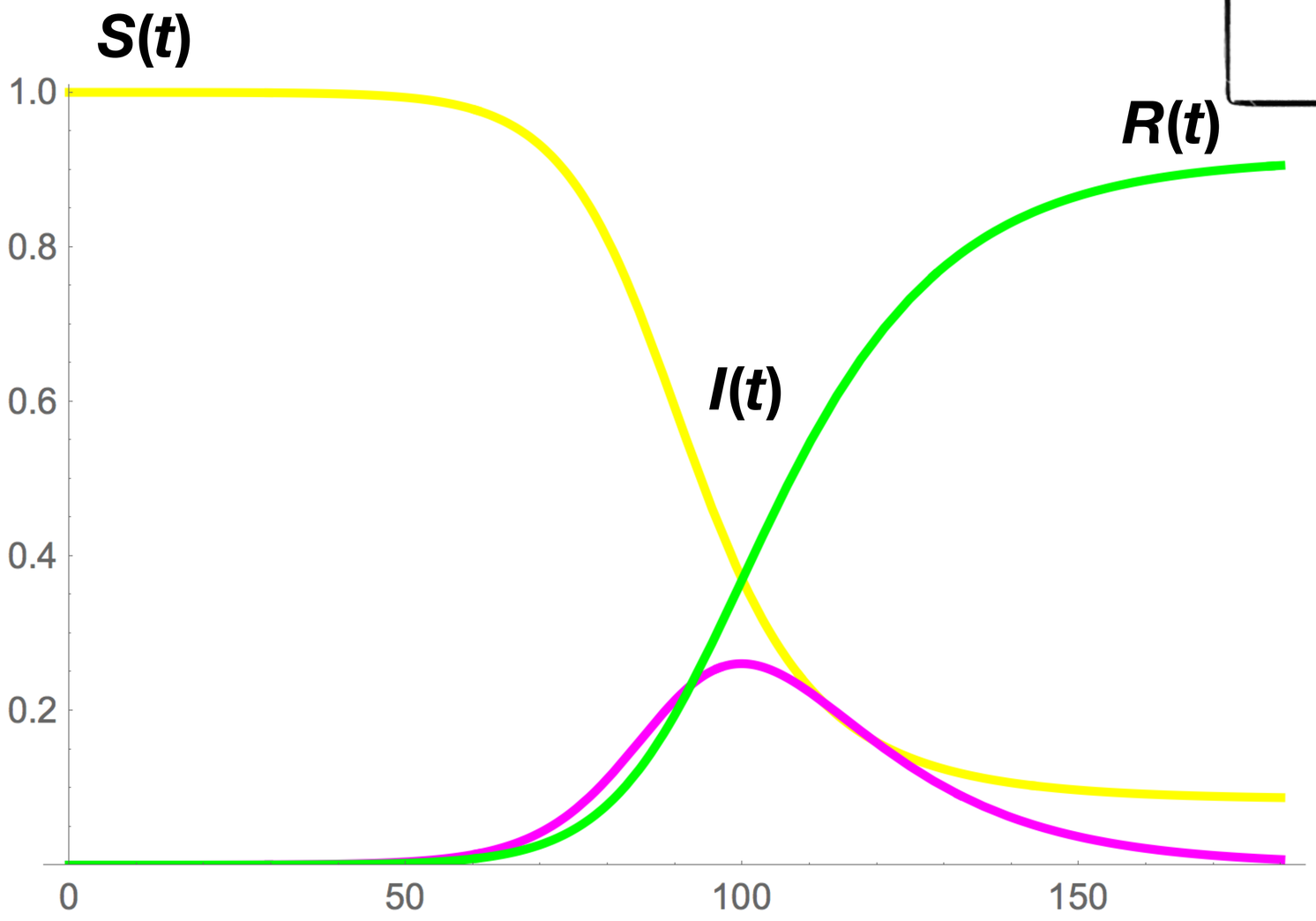


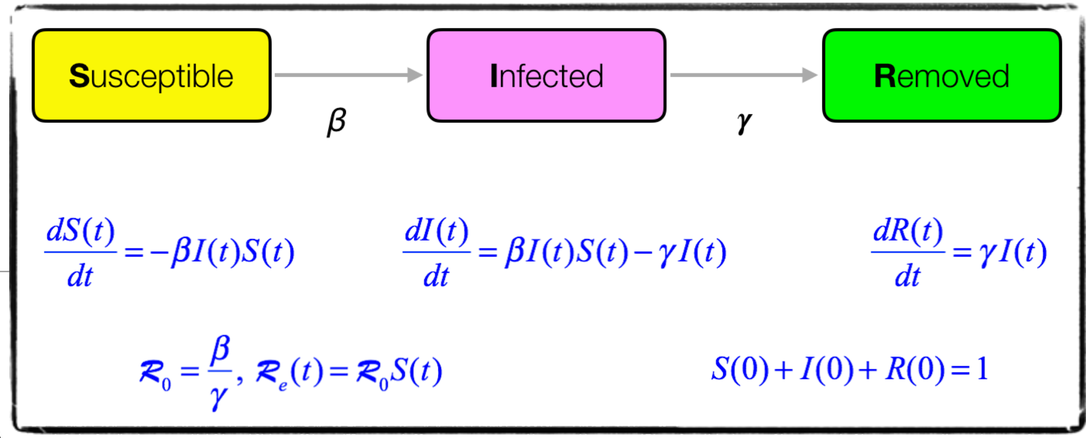
SIR Epidemic Model

$$\frac{dS(t)}{dt} = -\beta I(t)S(t) \qquad \frac{dI(t)}{dt} = \beta I(t)S(t) - \gamma I(t) \qquad \frac{dR(t)}{dt} = \gamma I(t)$$

$$\mathcal{R}_0 = \frac{\beta}{\gamma},\ \mathcal{R}_e(t) = \mathcal{R}_0 S(t) \qquad S(0) + I(0) + R(0) = 1$$

SIR Solution Example





$$\frac{dS(t)}{dt} = -\beta I(t) S(t) \qquad \frac{dI(t)}{dt} = \beta I(t) S(t) - \gamma I(t) \qquad \frac{dR(t)}{dt} = \gamma I(t)$$

$$\mathcal{R}_0 = \frac{\beta}{\gamma}, \ \mathcal{R}_e(t) = \mathcal{R}_0 S(t) \qquad S(0) + I(0) + R(0) = 1$$

$$I(0) = 10^{-5}$$

$$\beta = \frac{5}{26}$$

$$\gamma = \frac{1}{14}$$

$$\mathcal{R}_0 \doteq 2.69$$

Anti-Epidemic Interventions

transmission rate intervention ⬇

- moderating contact rate
- decreasing transition probability

removal rate intervention ⬆

- broad testing
- contact tracing

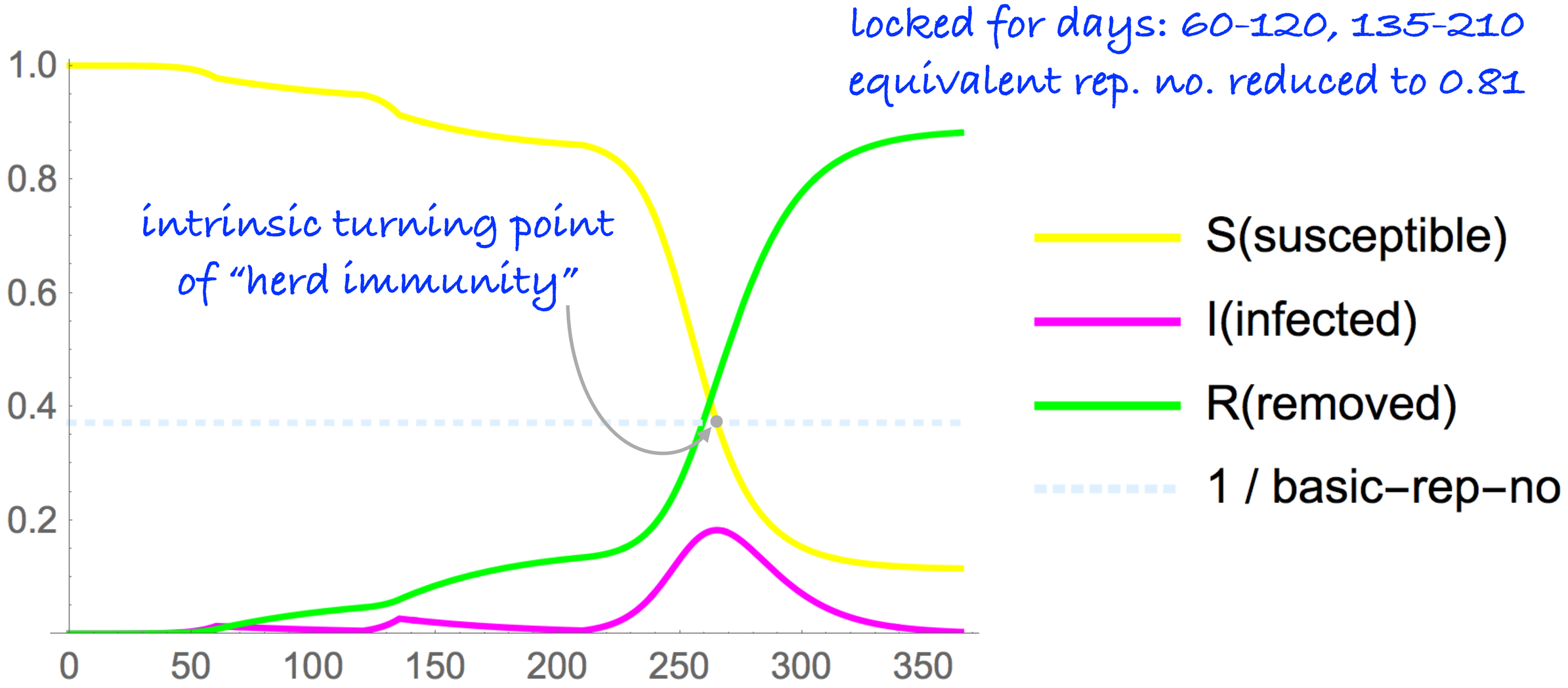
$$\frac{dS(t)}{dt} = -\beta I(t)S(t) \qquad \frac{dI(t)}{dt} = \beta I(t)S(t) - \gamma I(t) \qquad \frac{dR(t)}{dt} = \gamma I(t)$$

$$\mathcal{R}_0 = \frac{\beta}{\gamma},\ \mathcal{R}_e(t) = \mathcal{R}_0 S(t) \qquad S(0) + I(0) + R(0) = 1$$

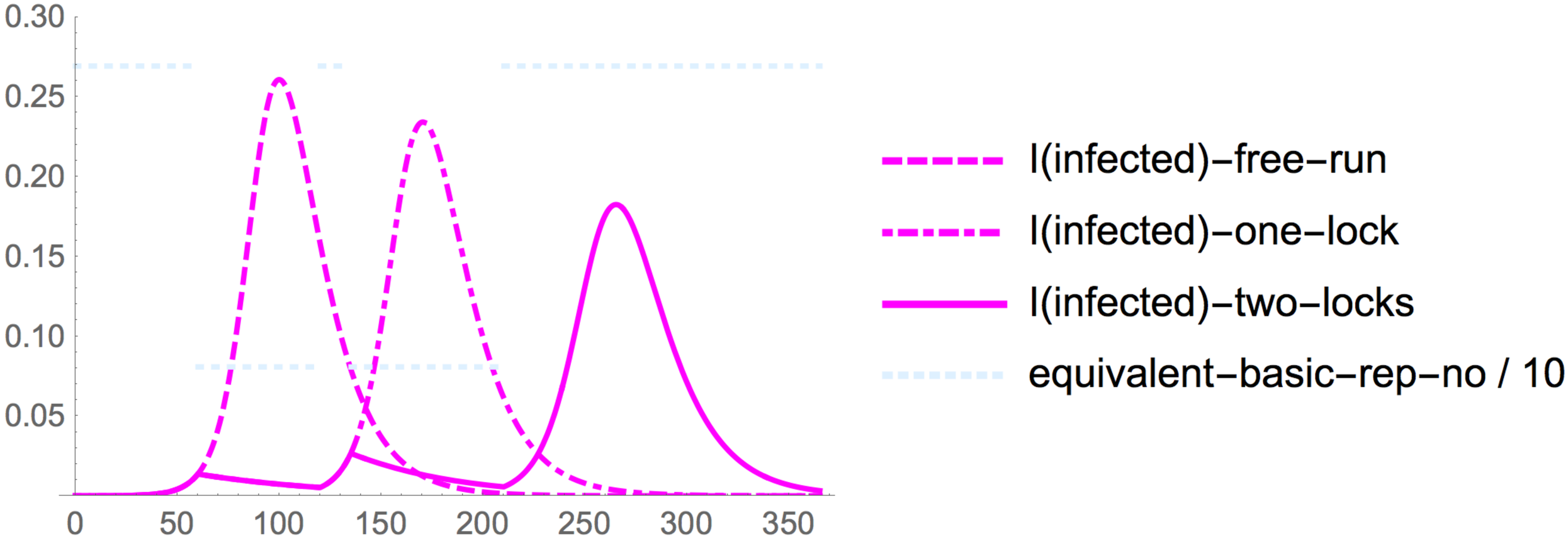
Understanding Mathematical Treatment

Primarily, it is not about the original cause.
The remedy can be a very tradeoff in between several factors.

Qualitative Study of Two Ideal Consecutive Lockdowns



Infected Compartment Comparative Close-Up



Let’s Talk About Strategy!

- There is a natural **intrinsic turning point** of the epidemic that is given solely by the *initial* basic reproduction number reciprocal (as the remaining susceptible fraction)
  - this point determines what we call *the herd immunity*
- Until we reach that point, the epidemic will by bouncing up and down with each and every lockdown release and reinforcement, respectively
- It is true that each and every wave following a (full) lockdown release will be milder in terms of its peak and the total number of people affected
- In principle, we could beat the epidemic this way
- The problem is, **relying solely on perpetual on/off lockdowns would take enormous amount of time, probably exhausting the state in other ways**

Bearable Countermeasure That Can Persist

- Apparently, we shall moderate the epidemic parameters permanently, not allowing them to relax back towards their free unmoderated values

  - this way, the intrinsic turning point is shifted (hopefully upwards) as well

- These countermeasure shall, however, last until the very end of the epidemic, so they shall be both **effective and bearable**

- **Reliable contact tracing and quarantine count in this!**

- Undoubtedly, vaccination is then an emergency wormhole that helps to skip a long track on the way to the intrinsic turning point; **we shall use it gratefully**

Conclusion

- **To safely return (not only) to our workspace,** we need to get COVID-19 (not only) in our offices under effective control

  ✅ enforce personal and environmental hygiene *(reduces transition probability)*

  ✅ moderate contact rate *(reduces meeting probability)*

  ✅ allow safe and secure one-to-one contact tracing followed by a quarantine, testing, and eventually the possible isolation *(increases removal rate)*

  ✅ take a vaccine whenever and as soon as possible *(turning point wormhole)*

Revision History

- 2020/12/16: initial version, simple SIR explanation included
- 2020/12/24: minor changes and the public release
- 2021/01/14: SIR-based lockdown effect explained (just qualitatively); the role of persistent countermeasures and vaccine noted
- 2021/02/09: herd immunity notion noted