Rump Session 2016

Oblivious Transfer from any non-trivial elastic noisy channel

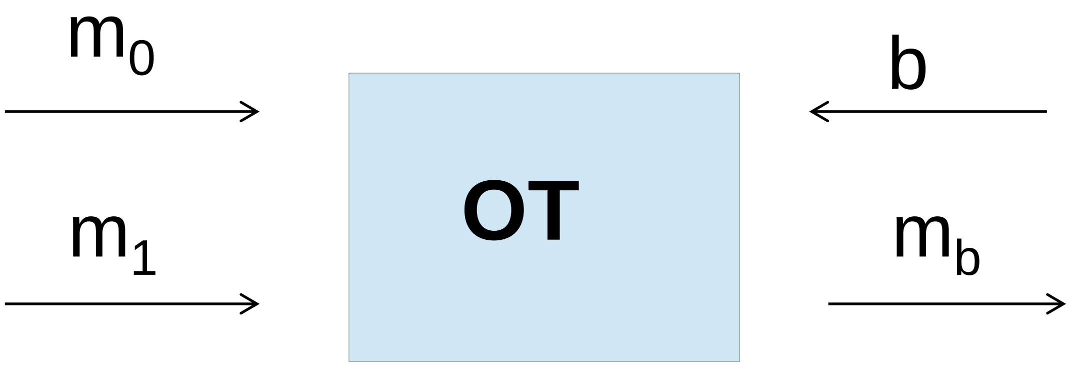
Ignacio Cascudo; Ivan Damgård; Felipe Larcerda; Samuel Ranellucci

Aarhus University

Oblivious Transfer

Sender

Receiver



m_0

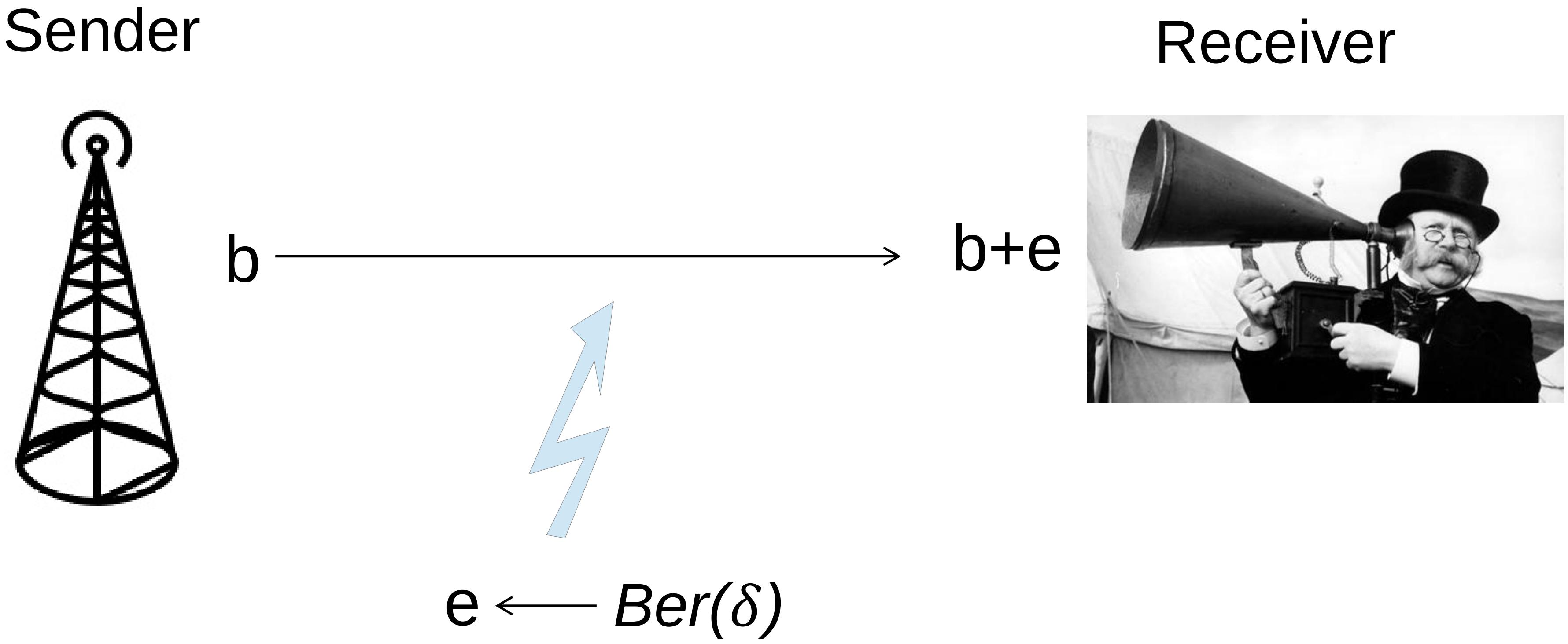
m_1

OT

b

m_b

Elastic noisy channel



Sender

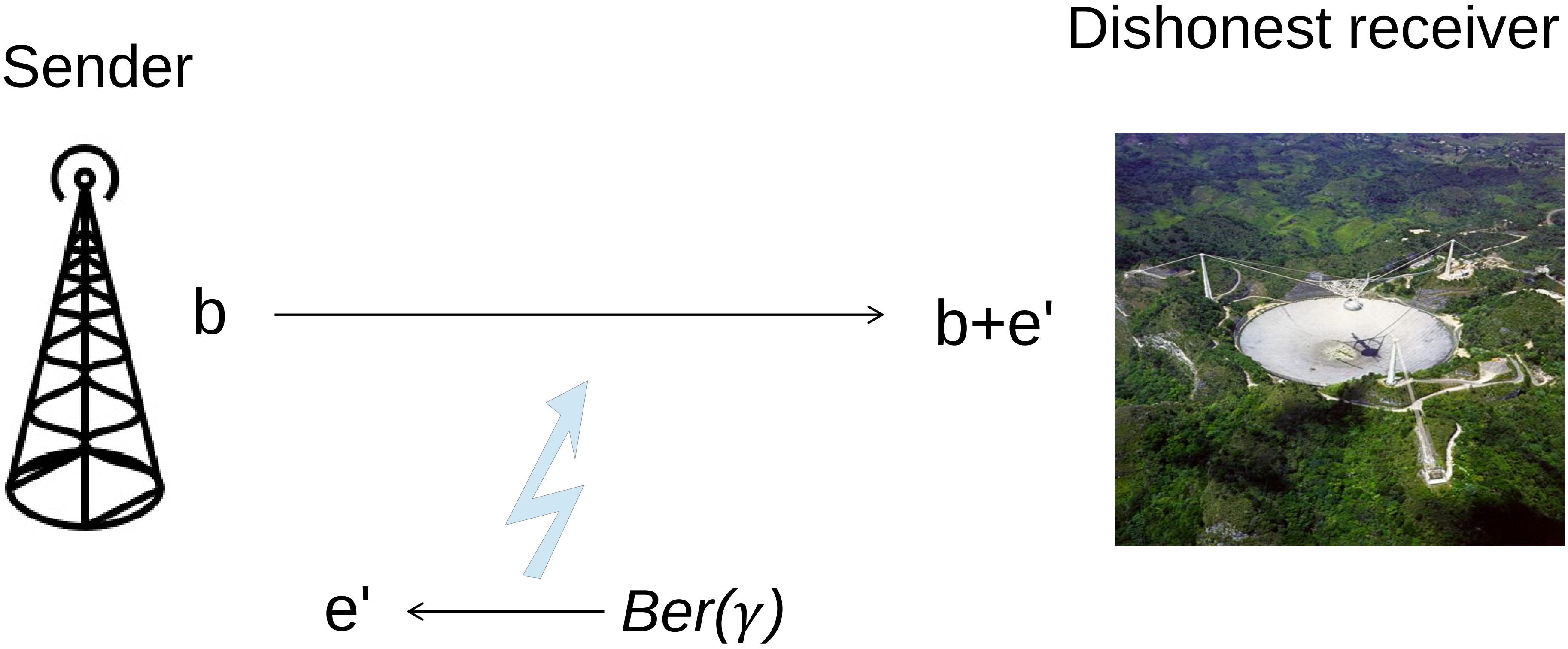
Receiver

b

b+e

e ⟵ *Ber(δ)*

Elastic noisy channel



Sender

Dishonest receiver

b

b+e'

e'

$Ber(\gamma)$

Model and previous result

- Secure Computation from Elastic Noisy Channels Dakshita Khurana, Hemanta K. Maji, Amit Sahai

- Result: OT is possible when

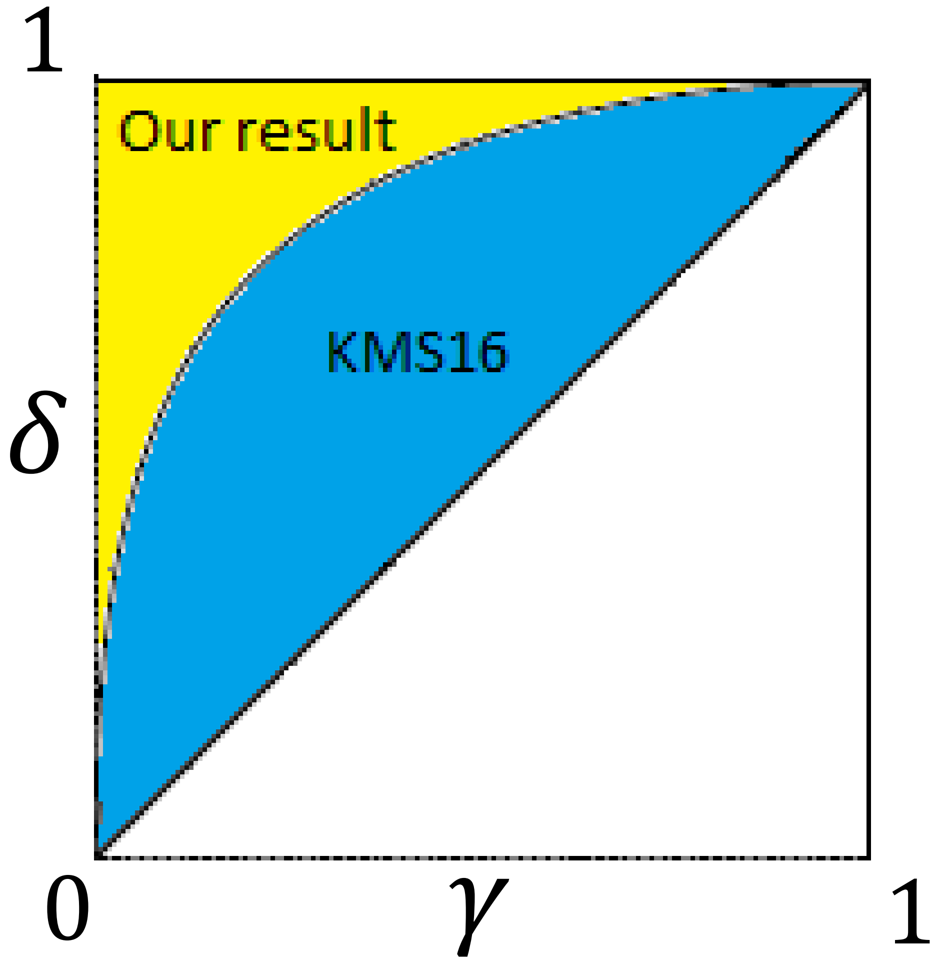
$$\delta \geq \left(1 + \left(4\gamma(1-\gamma)\right)^{-1/2}\right)^{-1}$$

Our result

- Result: OT is possible when

$$0 < \delta, \gamma < \frac{1}{2}$$

Comparison



Conclusion

- OT from any non-trivial elastic noisy channel
- http://eprint.iacr.org/2016/120
  - Report 120 (5!)
- Thank you for listening