To Mitigate Insecure Devices, Regulate Manufacturers or Consumers?

Tithi Chattopadhyay   Nick Feamster   Danny Yuxing Huang   **Matheus Venturyne**   S. Matthew Weinberg

{tithic,feamster,yuxingh,mvxf,smweinberg}@princeton.edu

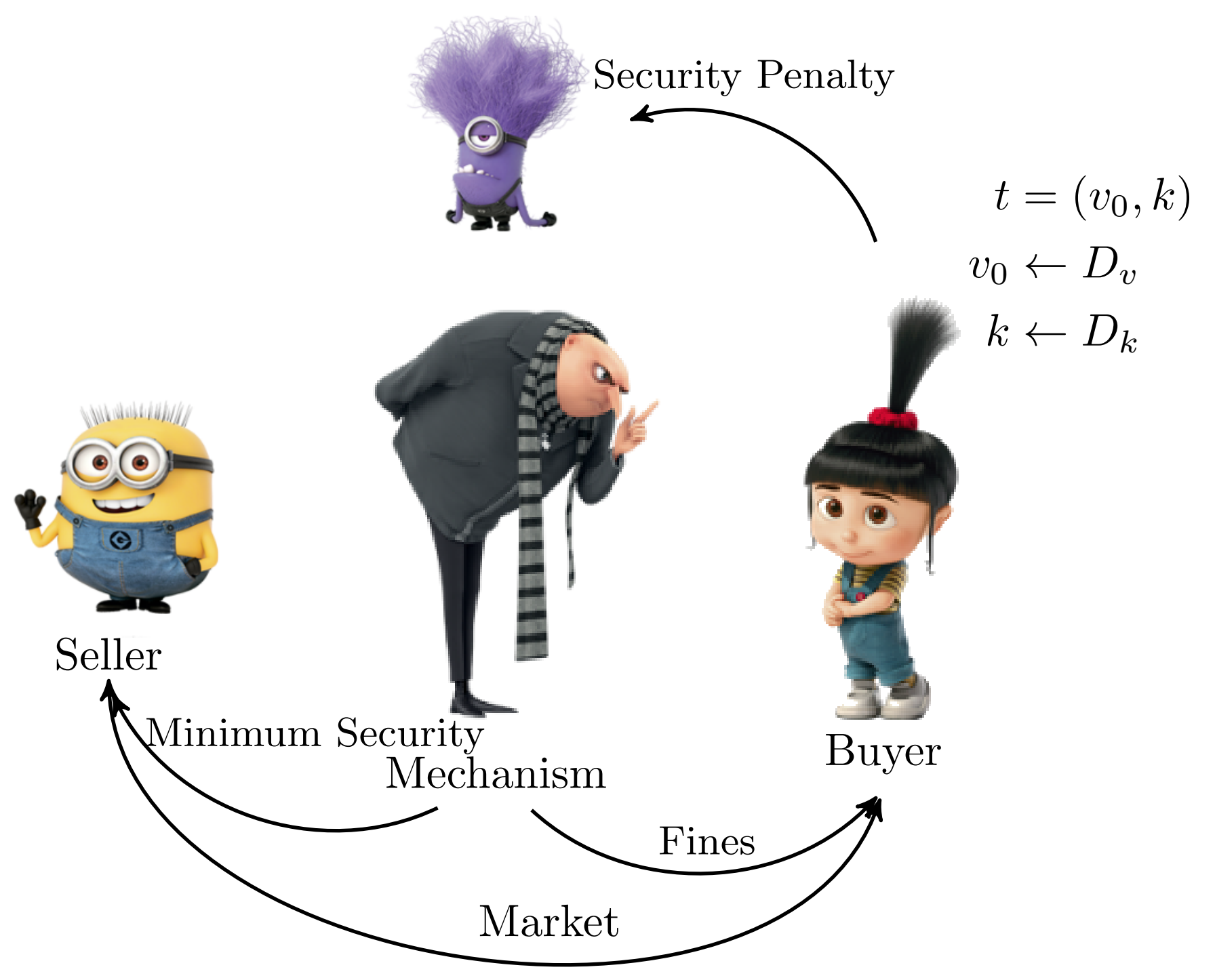
Objectives

Mitigating security vulnerabilities requires cooperation between consumers and manufactures. To mitigate the lack of incentives [2] [3], we propose a **Regulated Auction Mechanism** that regulates the manufacturers and/or consumers.

- We **require the manufacturers to enforce minimum security standards** for their devices — for instance, setting strong passwords or encrypting the network traffic.
- Alternatively, we increase consumers **privacy/security value** either by increasing their **consciousness** towards security or **fining owners** of devices which are compromised and used to attack other services on the Internet.

Our Method

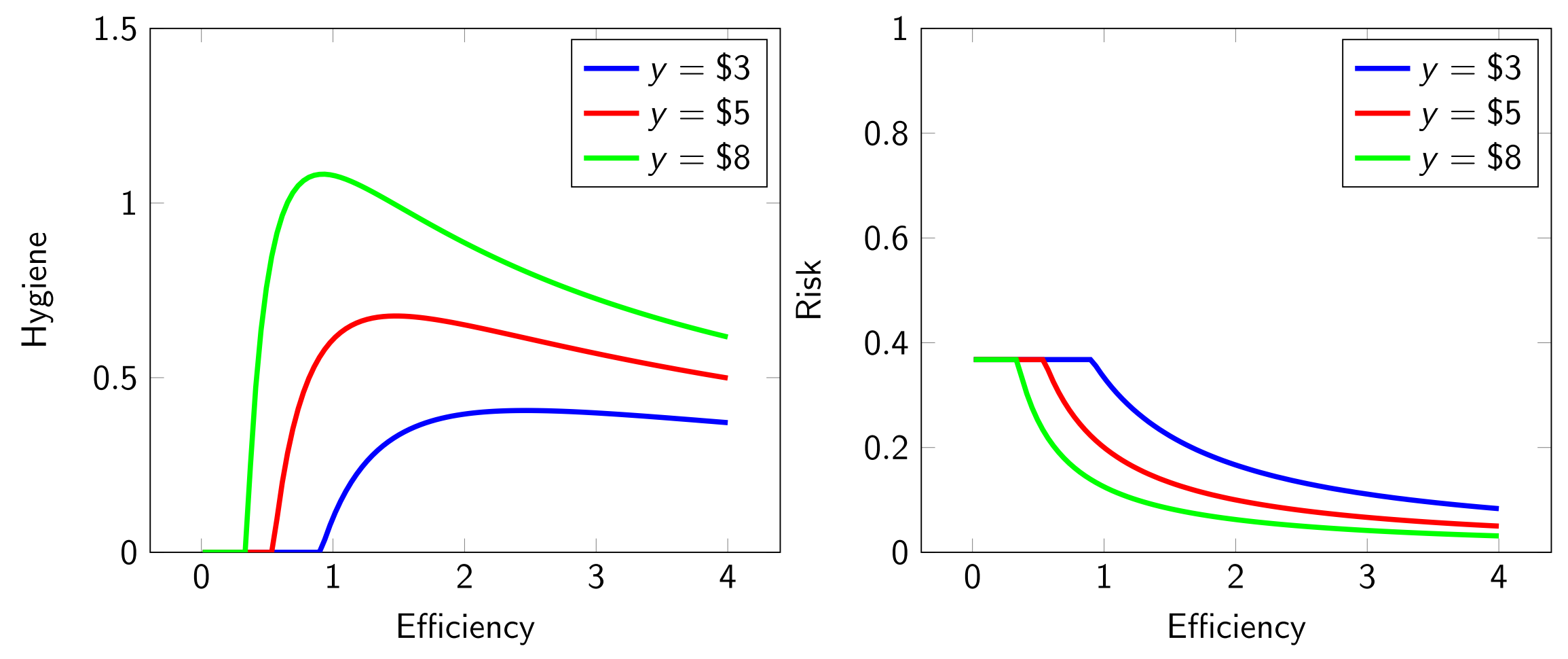
Manufacturers invest **minimum security**, incurring **costs** c. Under no regulation or security risks, consumers have a **prior value** v_0 drawn from distribution D_v. When a **fine** y is imposed over owners, consumers have incentive to mitigate their vulnerability which we denote by their **hygiene** h. The random variable k measures the **efficiency** of consumers in relation to manufacturers in mitigating security vulnerabilities.



$$risk = e^{-(\text{cost}+\text{efficiency}\cdot\text{hygiene})} \quad (1)$$

$$value = v_0 - \text{fine}\cdot\text{risk} - \text{hygiene} \quad (2)$$

$$Profit(D, p) = (p - c)\cdot Pr_{t\sim D}(v(t) \geq p) \quad (3)$$



Optimal Mechanism

The optimal mechanism selects a **policy** $s = (y, c)$ and a **price** p that minimizes the social risk, Equation 4, **constrained** on:

1. providing **minimum revenue** guarantees for the seller, Rev_0.
2. not reducing the buyer's **privacy/security value** y_0, $y \geq y_0$.

$$Risk(D, \pi, p, s) = \frac{\mathbb{E}_{t\sim D}(r(t,s)\pi(t))}{\mathbb{E}_{t\sim D}(\pi(t))} \quad (4)$$

Theorem: Optimal Simple Policies

A simple policy either regulates only consumers or only manufacturers. There is a cutoff δ such that

- For all efficiency distributions supported on $(0, \delta]$ either any regulation is infeasible or regulating only manufacturers is optimal.
- For all efficiency distributions supported on $[\delta, \infty)$ regulating only consumers is optimal.

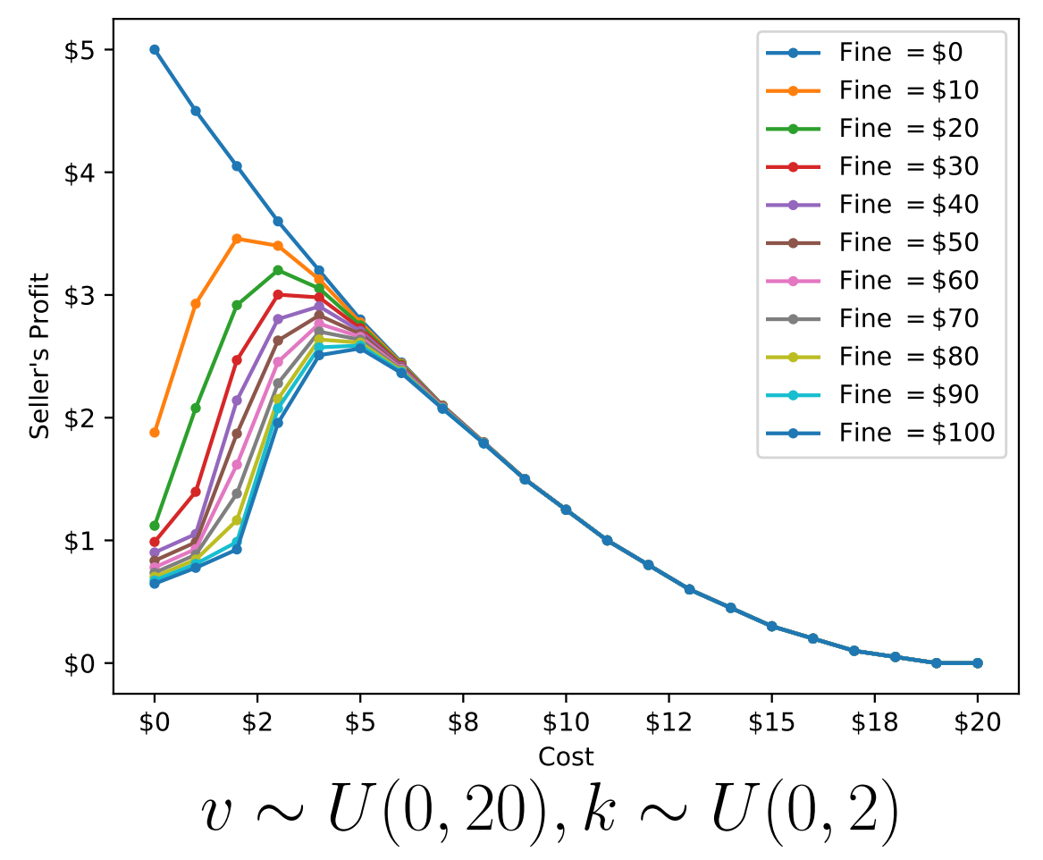
Proof Sketch: If a particular consumer has no incentive to minimize his own risk, then any less efficient consumers also would have no incentive to do so.

- For the mechanism, these types of consumers are indistinguishable.
- Since the consumers are inefficient, the mechanism is better of with regulating only manufacturers.

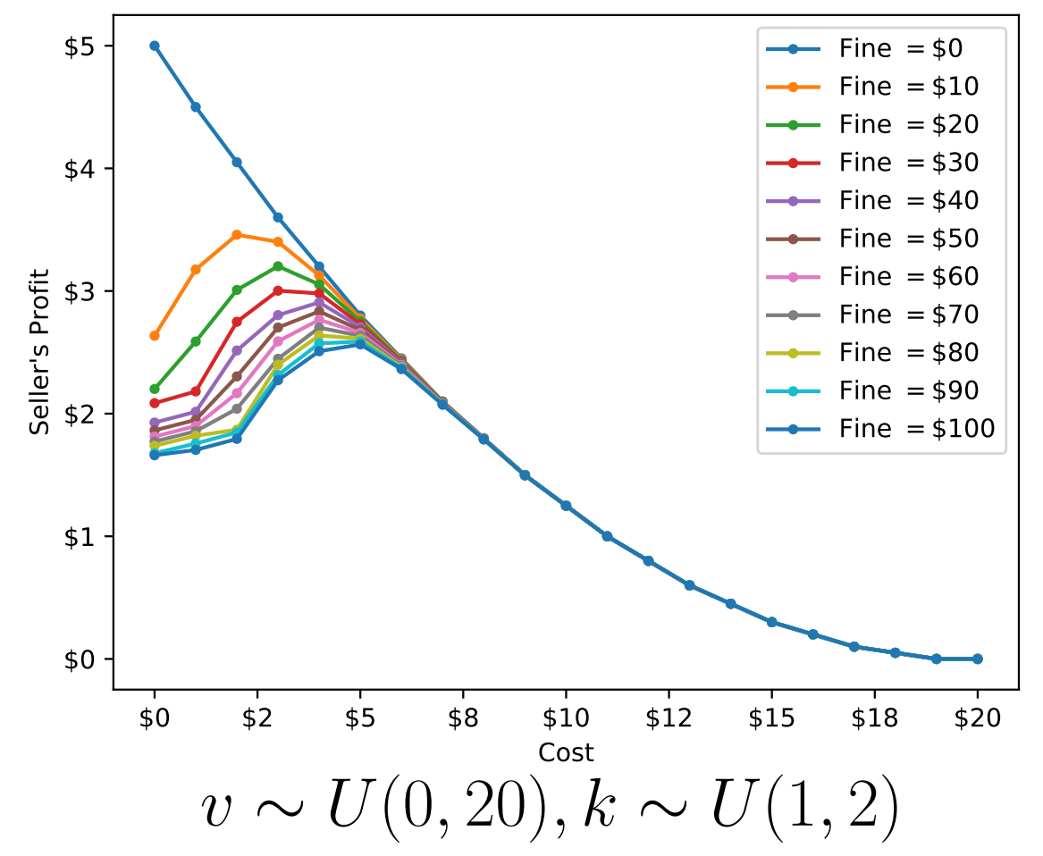
Similarly, if a particular consumer has incentive to minimize his own risk, then any more efficient consumers also would have incentive to do so. These consumers prefer policies with higher fines and lower production costs which cause

- Consumer's value to increase preserving their risk.
- The mechanism can charge higher prices and/or impose higher fines.

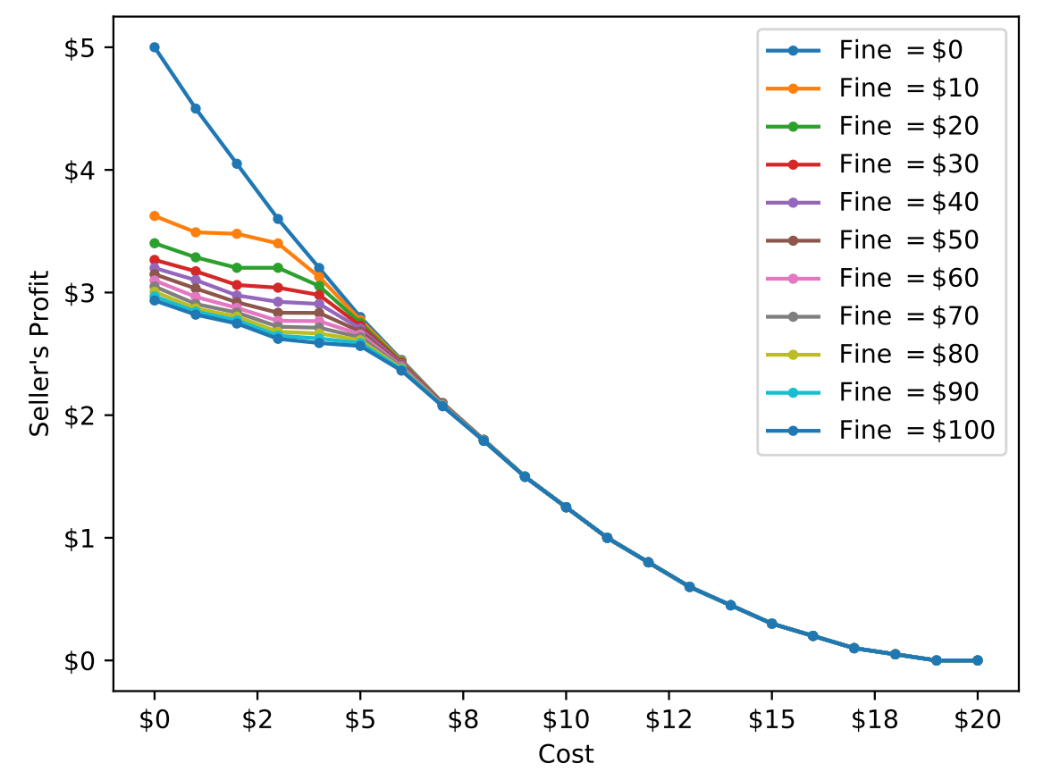
$v \sim U(0, 20), k \sim U(0, 1)$



$v \sim U(0, 20), k \sim U(0, 2)$



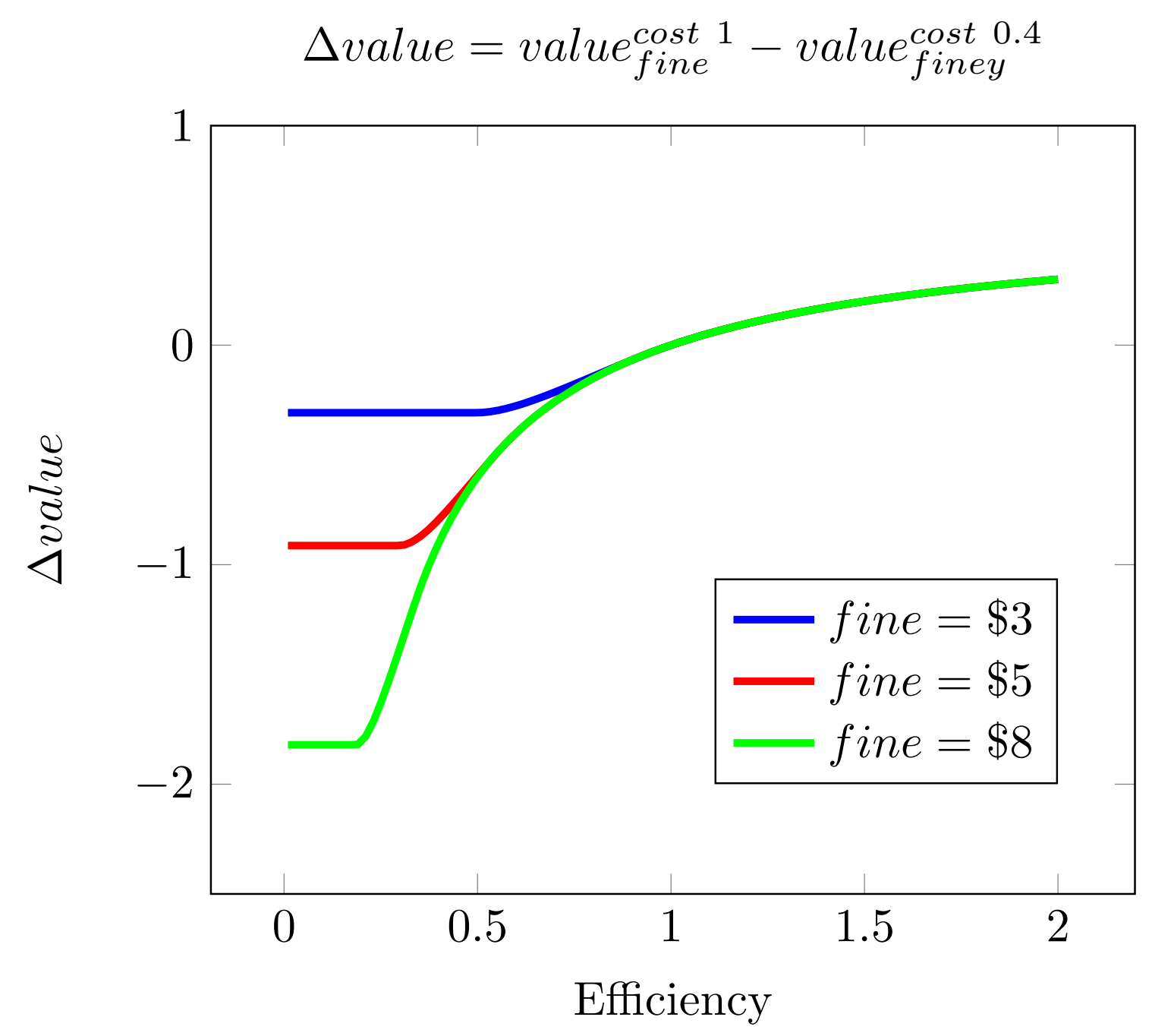
$v \sim U(0, 20), k \sim U(1, 2)$



Simple policies on general distributions

Under certain conditions, simple policies can provide good approximation for general distributions supported above and bellow the cutoff δ. Assume an arbitrary policy, then if ϵ is the probability of a consumer having no incentive to minimize his own risk under this policy, and if γ is an upper bound for the consumer's value without regulation, then

- Regulating only manufacturers is $\frac{1}{\epsilon}$-approximation for the risk.
- Regulating only consumers is e^{γ}-approximation for the risk.



The approximation ratio is tight; consider a scenario where

- Consumers have **high valuation** without regulation; ϵ fraction of the population is **inefficient** and $1 - \epsilon$ fraction is highly **efficient**.
- The mechanism has a **minimum revenue constraint** that can only be satisfied if everyone purchase the item. By constraining any feasible policy to sell to inefficient buyers, the social risk, Equation 4, can be made arbitrarily larger in comparison with the optimal policy.

Practical Consideration

To fit a real world scenario to our model, the prior value distributions should be rescaled. For example, suppose to reduce the risk of a cluster to 2% requires spending 80% of its value or \$80,000, then to fit this example to our model, we should rescale the clusters value to $\approx$ \$5, so that 80% of its value or \$4 reduces the risk to 2% $\approx e^{-4}$.

References

[1] Myerson, Roger B *Optimal auction design.* Mathematics of operations research (1981).

[2] August et al. *Market Segmentation and Software Security: Pricing Patching Rights.* WEIS (2016).

[3] Redmiles et al. *Dancing Pigs or Externalities? Measuring the Rationality of Security Decisions.* EC (2018).