Content identification

Yacov Yacobi
Microsoft Research
Keynote at 8th ACM DRM Workshop
October 27, 2008 Alexandria, VA, USA

Contour

General

1. Physical Vs. digital goods,
2. Classic DRM
   a. Before the fact,
   b. After the fact,
      (i) Fingerprints,
      (ii) Traitor tracing,
3. *New DRM.*

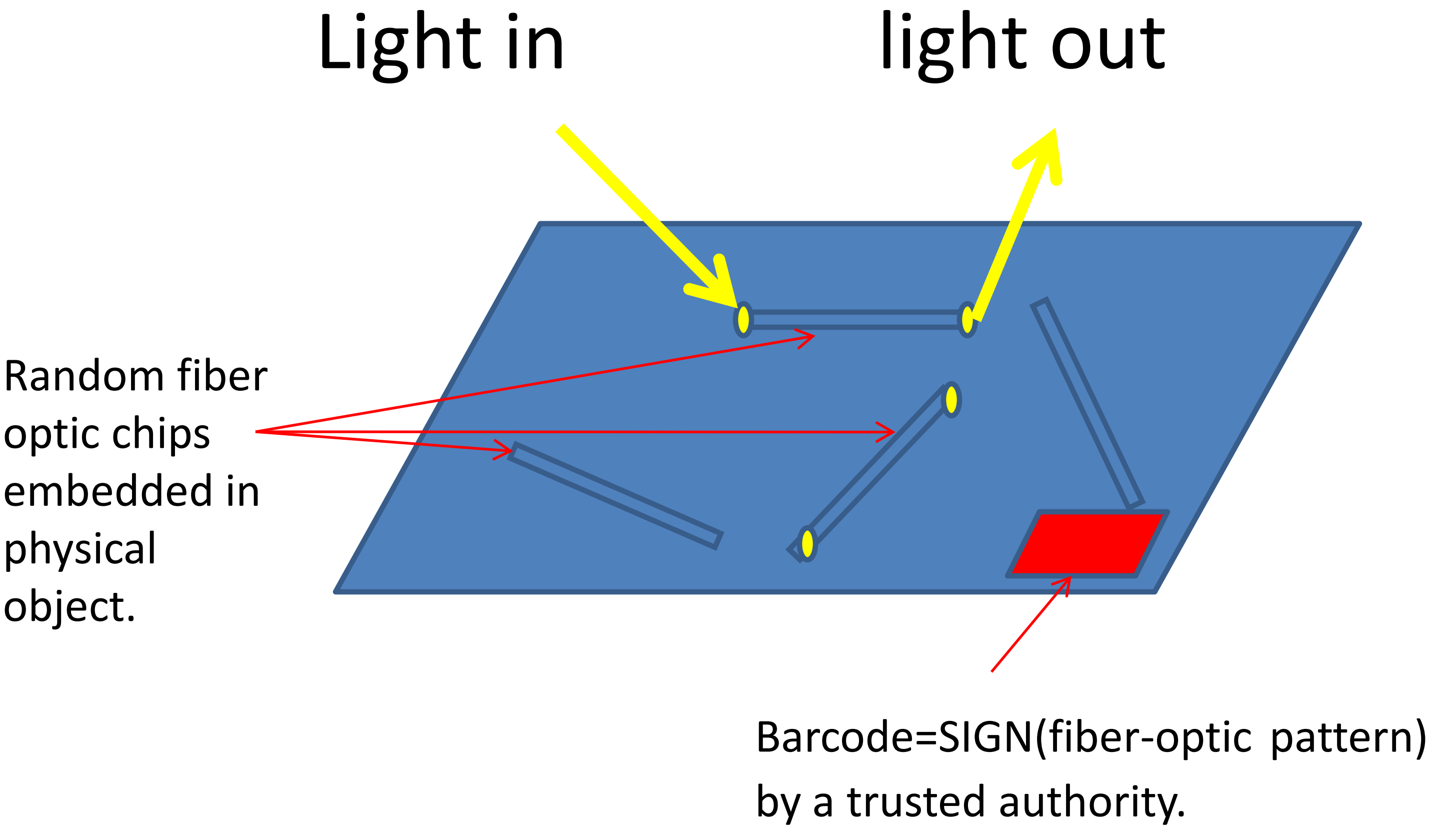
Today's talk

1. Speculate about new DRM,
2. Economics
   a. Piracy
   b. *Counterfeiting*

Damage from Counterfeiting

1. World Economic Forum: Damage from counterfeiting went from $430b in 2004 to $3t in 2007.
2. Physical counterfeiting (medicine, aviation parts, etc.). Solution: *Don Bauder & Gus Simmons* of Sandia National Labs, SALT agreement, 70's.

Physical counter counterfeiting (Bauder & Simmons)



How good can it possibly get?

(new DRM)

DRM for web hosting (“the new DRM”):

Web-host shares ad-revenues w/producer.

Identify the true producer.

Comparison

- The new DRM problem is easier to solve than the classic one. It enjoys numerous *systemic* advantages.

- In addition, replacing watermark technology with media-*hashing* has *operational*, *computational* complexity, and *robustness* advantages.

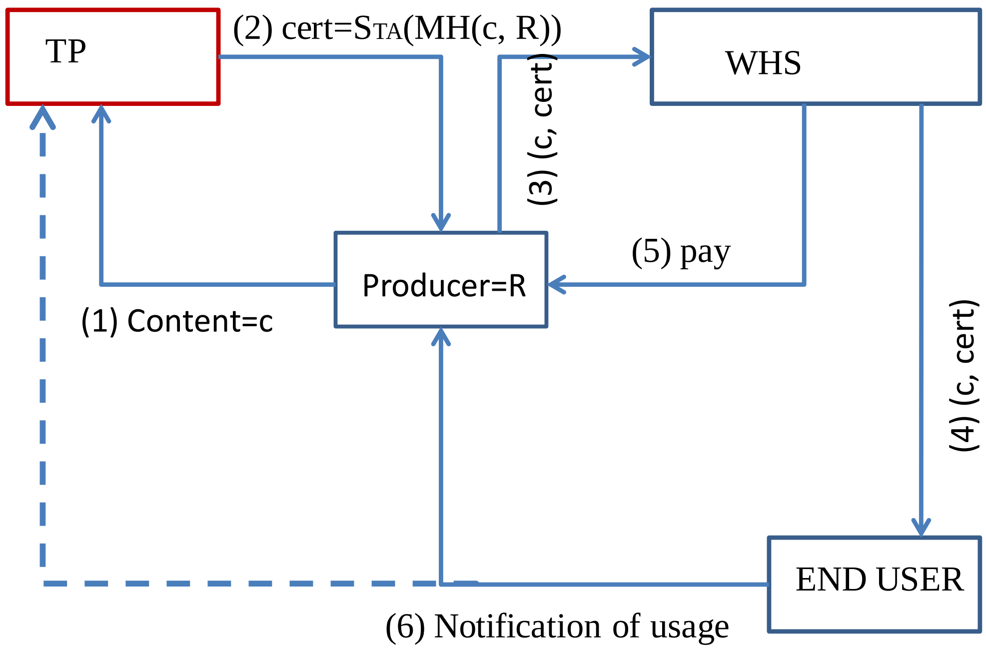
Media hashing

- *Objects* $Ci \cong Cj \rightarrow h(Ci)=h(Cj)$.

  [Ref.: M.H. Jakubowski; M. K. Mihcak; R. Venkatesan]

- Creator *R* created object *c*.
- A ***trusted*** party *TP* issues a certificate $cert=SIGN_{TP}(h(c),R)$, if it hasn't seen $h(c)$ before.

A possible new DRM system



TP=trusted party,
WHS= Web hosting service,
MH=Media hash,
S_{TA} (m)=Signature of TA on m.

Fig. 1: Ad-based revenue generation using media hashing to control fraud.

Systemic advantages of new DRM

- End user is not the enemy;
- Attacker does not know the secret key, and cannot even experiment with the decoder as a black box;
- The assumption that end-user does not modify her player is realistic (since she is not a side in this struggle).

Advantages of hashing over marking

- Operational: Protects the *past*.
- Complexity & Robustness: By def. more efficient & more robust ($\in$ watermarking),
- Example: current image-hash tolerate $\pm 20^0$ rotations. For images, 360/(2*20)=9 trials are enough. For video, after $\pm 20^0$ rotations it is not valuable, so 1 trial.

How good is good enough?

(classic DRM)

REFERENCES

- Banerjee, D.S., 2003, 2006 (“piracy..”),
- YY & Gideon Yaniv in this proceedings.

Counterfeiting Vs. Piracy

- CF looks like original, costs like original, and counterfeiter competes against legal producer in the same market.

Setting

- **Def.:** q = probability to correctly trace (eg, using sting ops), successfully prosecute, and penalize a counterfeiter.

- **Q:** What is the payoff of improving q?

Over simplifications

- Counterfeiter mimic original w/out costs,
- Consumers pay full price for counterfeits,
- Everybody is economically rational.

Reasonable Assumptions

1. Once traced & successfully prosecuted there is a fixed proportion 1/γ between crime and punishment.

2. Audit events are independent,

3. Probability of false positives is negligible (adjust threshold accordingly).

Notations

- x=# illegal copies,
- q=Pr[detection after a single illegal copy],
- $q=\alpha\beta$,
- $\pi(x)$=Pr[det. after x copies]=$1-(1-q)^x$,
- p=price of a copy,
- F=$ punishment,
- $\gamma=F/xp=punish/crime$,
- $P(x)$= gain of the CF,

  $=(1-\pi(x))px- \pi(x)F$
- x^* = optimal CF production,
- Lambert : $L(z)e^{L(z)} = z$,
- $\lambda(\gamma) = L(e \cdot \frac{\gamma}{1+\gamma}) - 1.$

More precisely

$$x^* = \min\{D(p)/n, \frac{\lambda(\gamma)}{\ln(1-q)}\}$$

Market size at price *p*

Number of independent counterfeiting groups.

Henceforth we ignore boundary conditions, and some other details, assuming $x^* < D(p)/n$, and $q > 0$.

The Counterfeiter

Theorem 1:

$$(i)\ \ x^{*} = \lambda(\gamma)/\ln(1-q) \approx -\lambda(\gamma)/q,$$

$$(ii)\ P(x^{*}) > 0,$$

$$(iii)\ \pi(x^{*}) = 1 - e^{\lambda(\gamma)}.$$

i.e. $\pi(x^{*})$ is independent of q and p.

It depends only on γ.

Corollary : $\pi(x_{w}^{*}) = \pi(x_{o}^{*})$.

The economics of the protection

- n=# counterfeiters.
- Subscripts *w,o* denote parameter values *w*ith and with*o*ut improvement (technological, or audit rate),
- For $i \in \{w,o\}$ R_i = revenues of legal producer.
- $P_2 = R_w - R_o$ = payoff of legal producer due to improvement.

Payoff of the legal producer

$$R_w = (D(p) - x_w^*)\,p; \quad R_o = (D(p) - x_o^*)\,p,$$

$$P_2 = \mathrm{R_w} - \mathrm{R_o},$$

For a single counterfeiter:

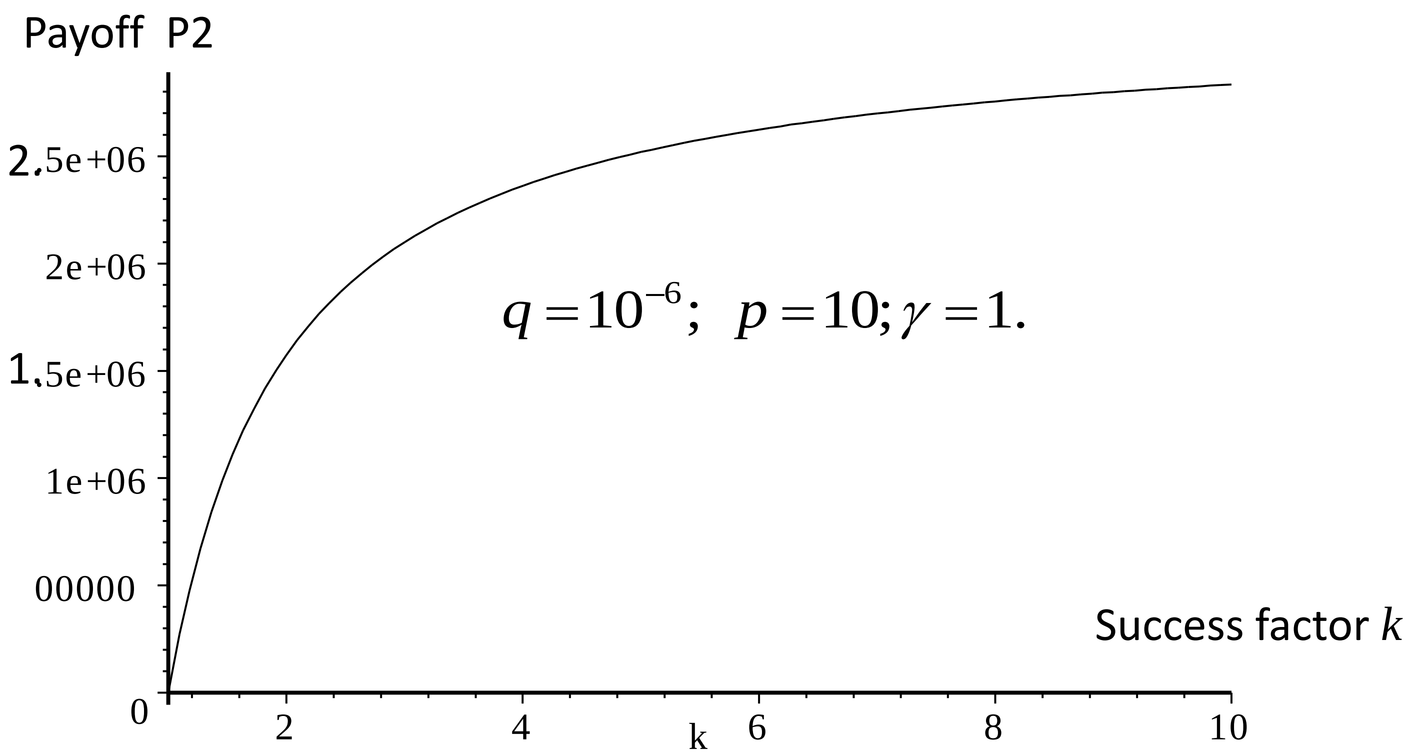
$$P_2 = \lambda(\gamma)\,p\left(\frac{1}{\ln(1-q_o)} - \frac{1}{\ln(1-q_w)}\right),$$

For n counterfeiters:

$$P_2 = \lambda(\gamma)\,np\left(\frac{1}{\ln(1-q_o)} - \frac{1}{\ln(1-q_w)}\right).$$

Success factor $k = q_w / q_o$.

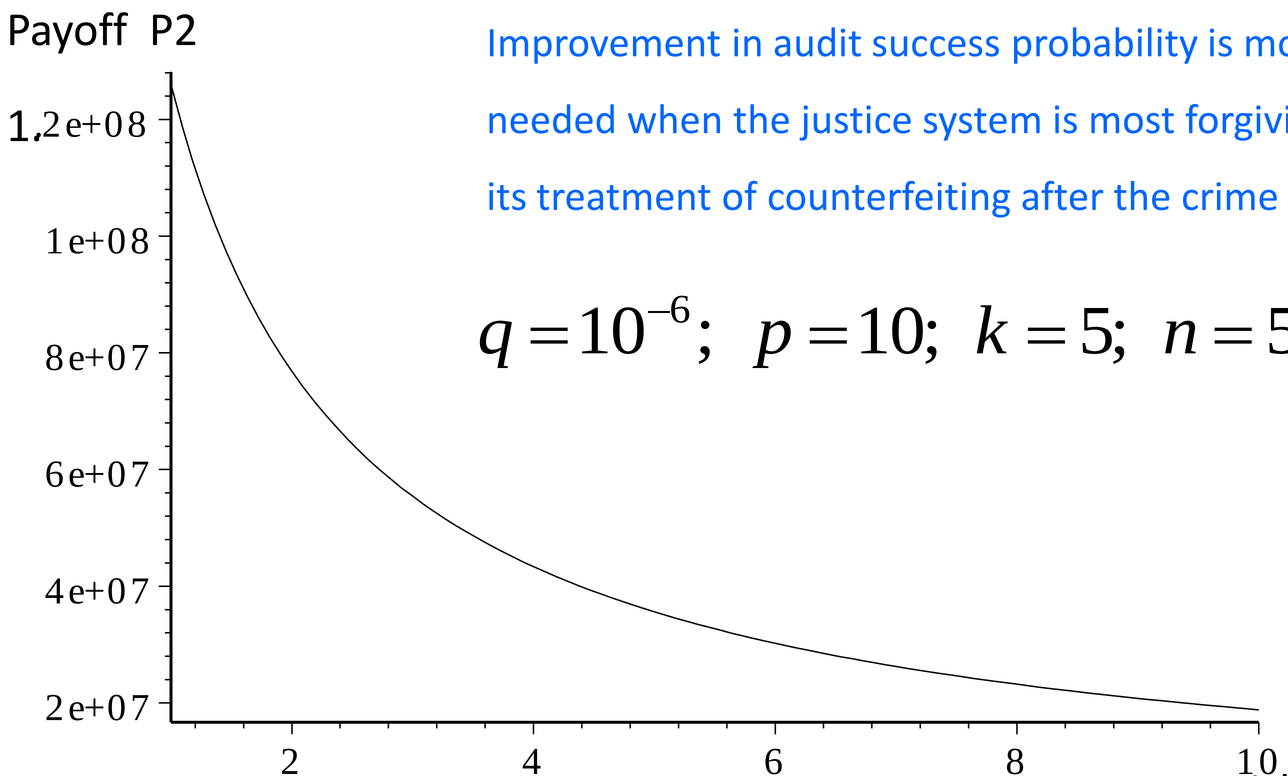
Freeze γ variable k



$$q = 10^{-6}; \quad p = 10; \gamma = 1.$$

K=5 captures most of the payoff (re, how good is good enough).

Freeze k variable γ



Improvement in audit success probability is most needed when the justice system is most forgiving in its treatment of counterfeiting after the crime has been proven.

$$q = 10^{-6};\ \ p = 10;\ \ k = 5;\ \ n = 50$$

$$\gamma = \frac{\text{Punishment}}{\text{crime}}$$

Max # counterfeiters

n counterfeiters crowd the market; each gets $x=D(p)/n<x^*$

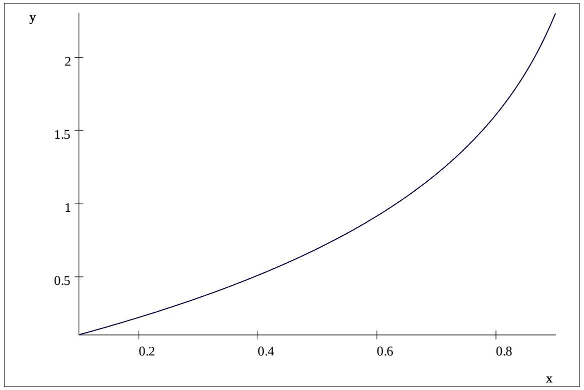
$$\text{Claim}: \quad n_{\max} = \frac{D(p)\ln(1-q)}{\ln(\frac{\gamma}{1+\gamma})}$$

$$\text{Proof}: \ (1-\pi(D/n))\,pD/n - \pi(D/n)F = 0,$$

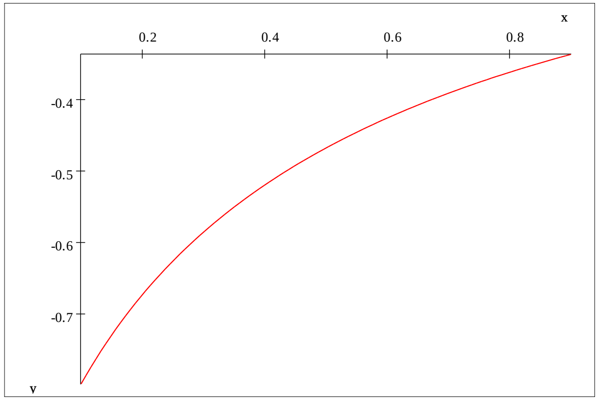
$$F = \gamma pD/n.$$

APPENDIX

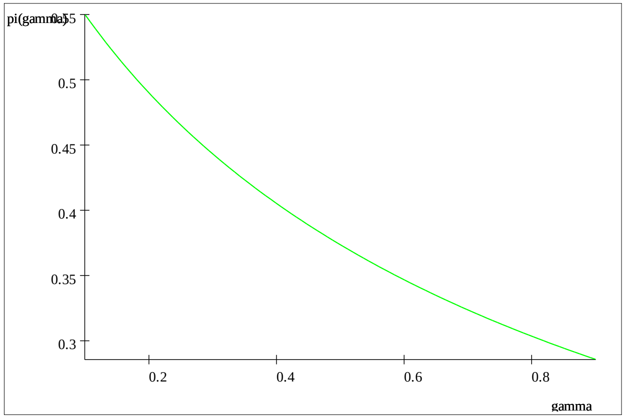
$-\ln(1-q)$



$\lambda(\gamma) = \text{LambertW}(e * \gamma/(1+\gamma)) - 1$



$$\pi(x^*) = 1 - e^{\lambda(\gamma)}$$



$\gamma = 1/2$

$$\frac{n_{\max}}{D} = \frac{\ln(1-q)}{\ln(\gamma/(1+\gamma))}$$