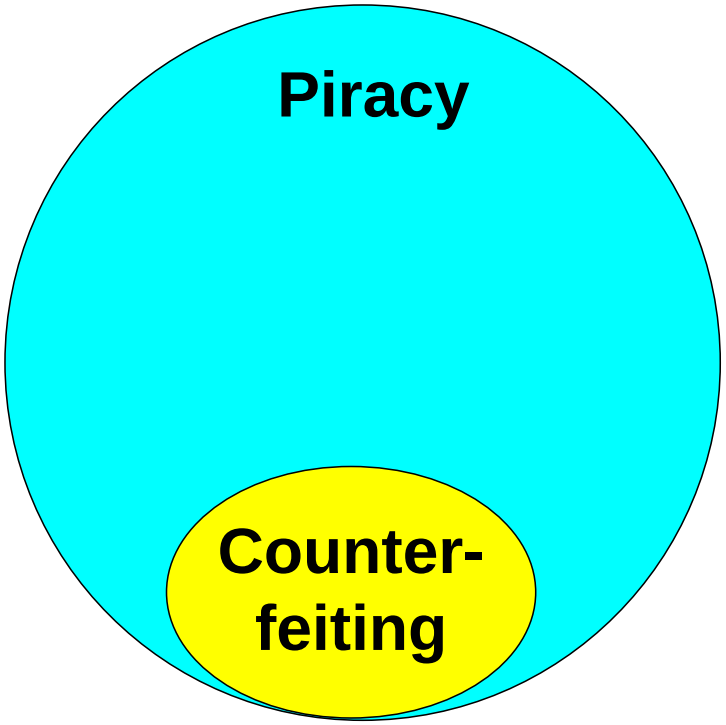
# Optical DNA

Deepak Vijaywargi, University of Washington
Dave Lewis, Microsoft Anti-Piracy Team
Darko Kirovski, Microsoft Research




- Piracy
  - Buyer knows product is not genuine
- Counterfeiting
  - Seller tricks buyer into believing product is genuine

# Why Optical Media?

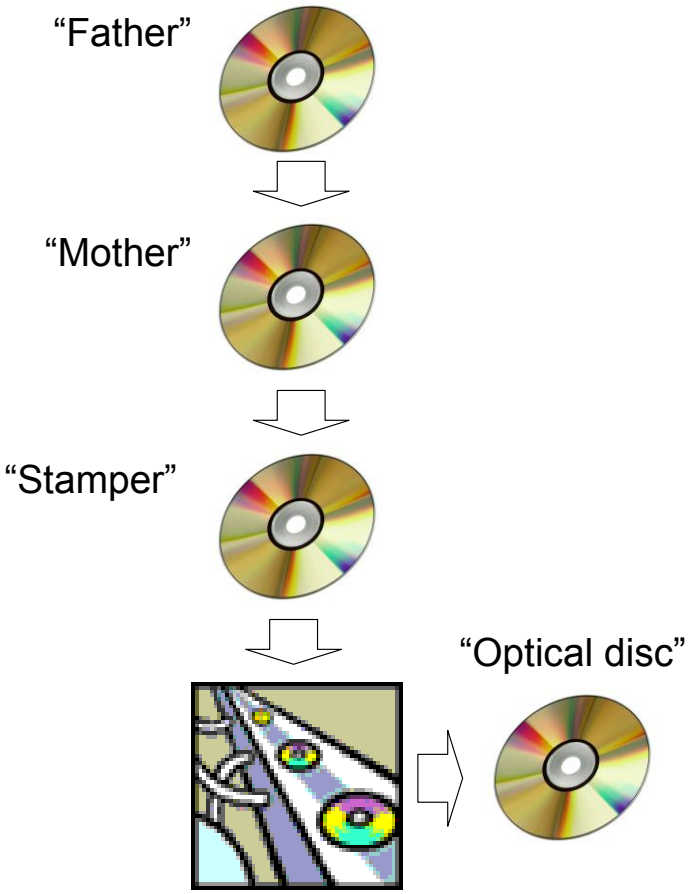
- Quite a bit of value to protect
  - US ($21B + $40B + $132B) / year
- Blu-ray 50GB = US$1-2
- 9.5GB = US 50¢
  - US$ $5.31 \cdot 10^{-11}$/byte
  - Download the same data, 3Mbps
    - US 11.5¢/kWh[1], 50-300W laptop-desktop
    - US 4-24¢ (energy) + US 7¢ (cable service)

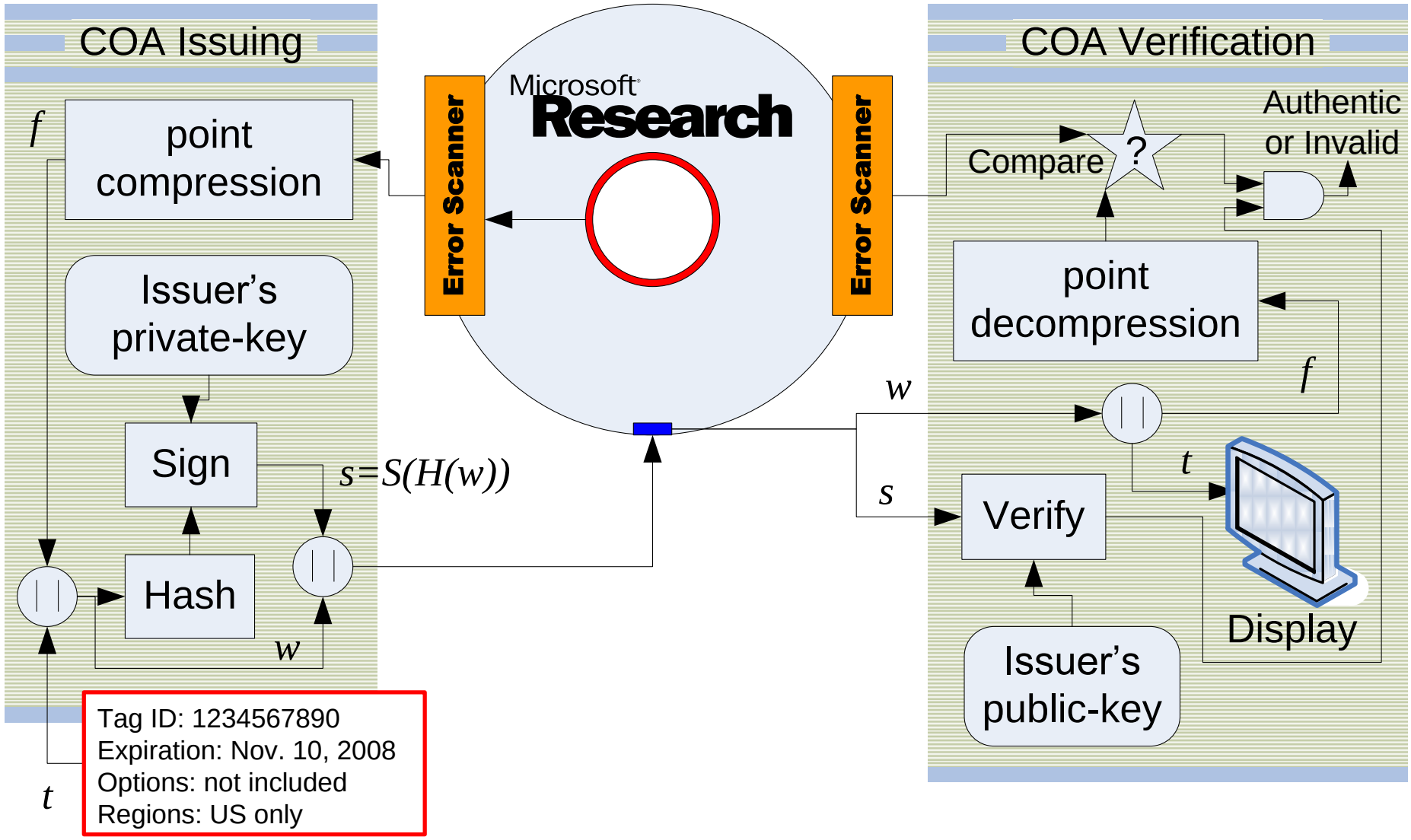
# Certificate of Authenticity

- Bauder and Simmons, Sandia Labs
- Optical DNA: hedge over RF-DNA
- Physical object
  1. Unique randomness
  2. Expensive to create a near-exact replica
  3. Inexpensive to manufacture
  4. Inexpensive to scan the random structure
  5. Inexpensive signing and verification
  6. Robust to wear and tear

# Source of Randomness

- Manufacturing errors inevitable
- No errors $\Rightarrow$ poor density
- Latest standard will always be a source of errors
- TechniColor
  - DVD = $0.40
  - Hologram = $0.25




COA Issuing
f
point compression
Issuer's private-key
Sign
s=S(H(w))
Hash
w
t
Tag ID: 1234567890
Expiration: Nov. 10, 2008
Options: not included
Regions: US only
Error Scanner
Microsoft Research
Error Scanner
w
s
COA Verification
Compare
?
Authentic or Invalid
point decompression
f
t
Verify
Display
Issuer's public-key

# The Errors

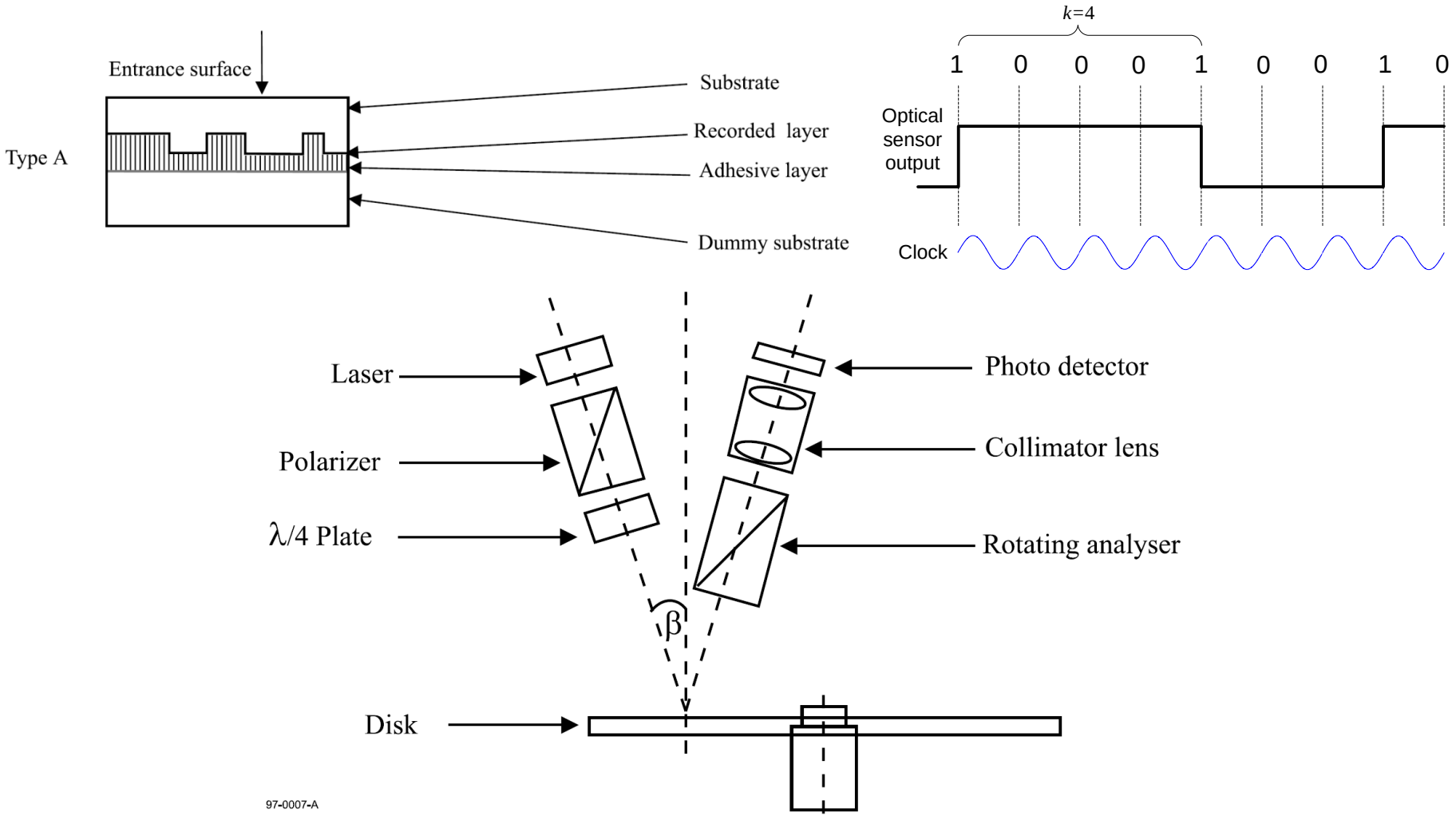
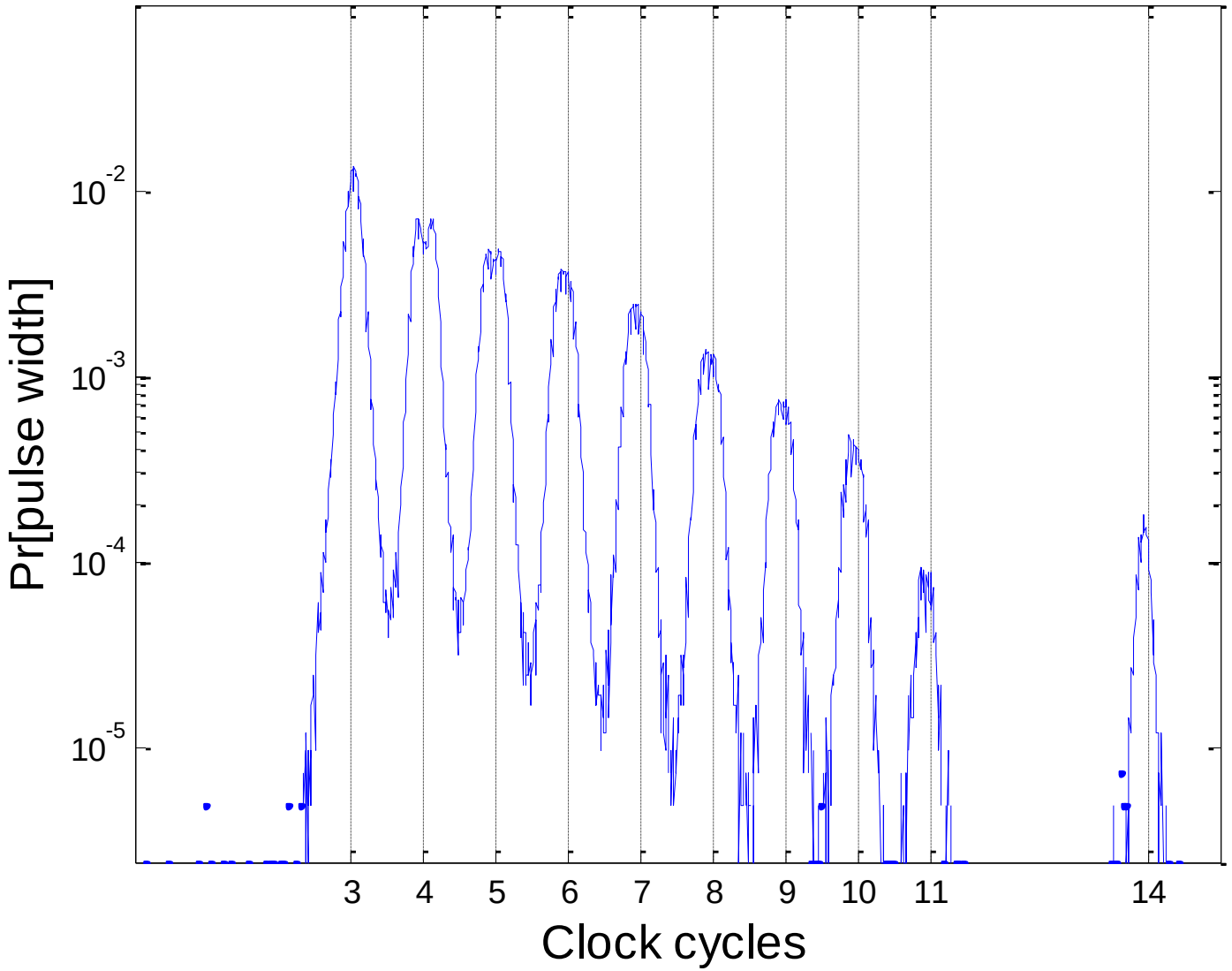



**Figure B.2 - Example of a device for the measurement of birefringence**

Standardizing Information and Communication Systems. 120 mm DVD – Read-Only disc. Standard ECMA-267. 3rd Edition, 2001.

# Pit/Gap Length



# Error Classes

- $e_1$ – on all discs made by the same stamper…
- $e_2$ – unique deterministic errors
- $e_3$ – probabilistic errors
  - Need multiple reads to identify them
  - pit = 3.5 clock cycles long
- $e_4$ – wear and tear

# Upper Level of Encoding

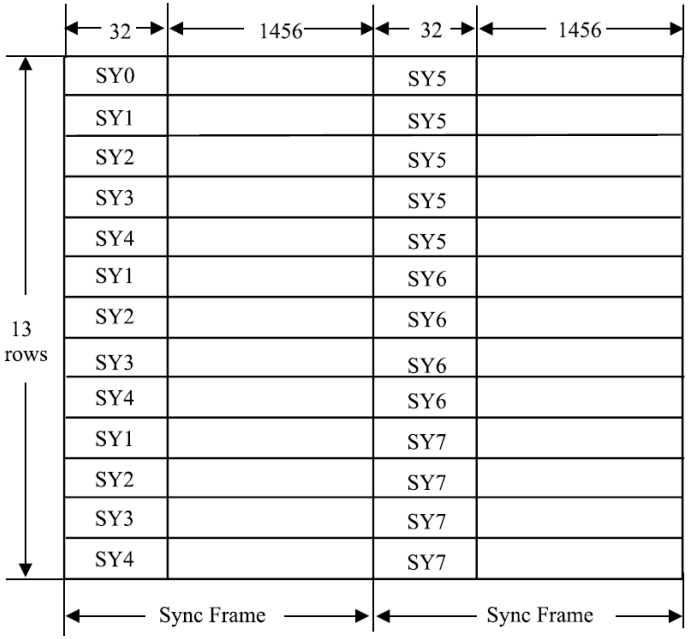


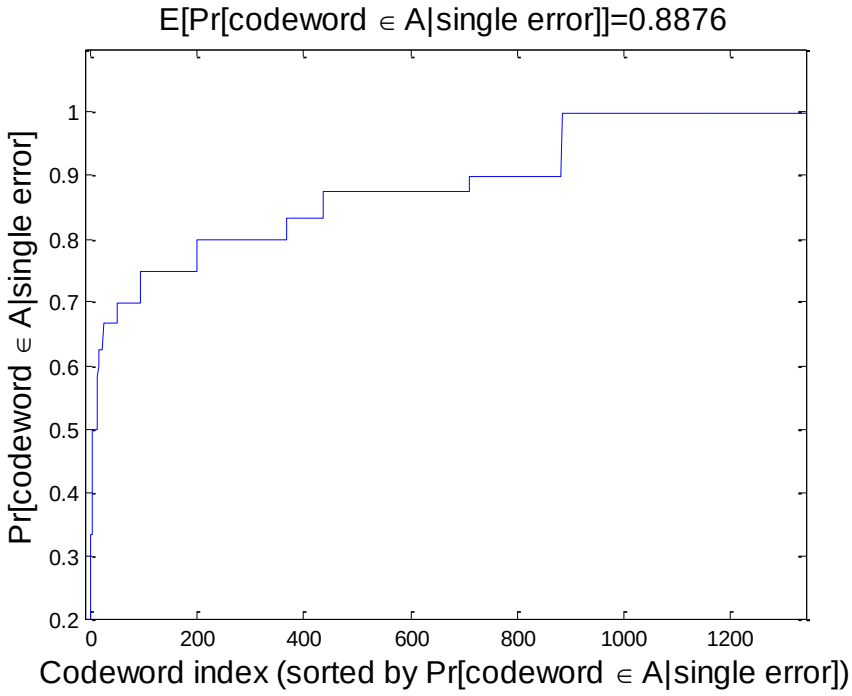

**Table G.1 - Main Conversion Table**

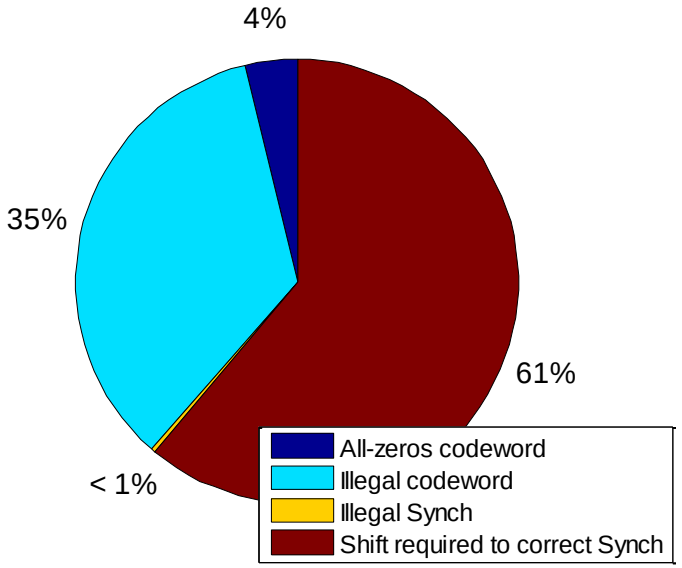
| 8-bit byte | State 1 | | State 2 | | State 3 | | State 4 | |
|---|---|---|---|---|---|---|---|---|
| | Code Word msb lsb | Next State | Code Word msb lsb | Next State | Code Word msb lsb | Next State | Code Word msb lsb | Next State |
| 0 | 0010000000001001 | 1 | 0100000100100000 | 2 | 0010000000001001 | 1 | 0100000100100000 | 2 |
| 1 | 0010000000010010 | 1 | 0010000000010010 | 1 | 1000000100100000 | 3 | 1000000100100000 | 3 |
| 2 | 0010000100100000 | 2 | 0010000100100000 | 2 | 1000000000010010 | 1 | 1000000000010010 | 1 |
| 3 | 0010000001001000 | 2 | 0100010010000000 | 4 | 0010000001001000 | 2 | 0100010010000000 | 4 |
| 4 | 0010000010010000 | 2 | 0010000010010000 | 2 | 1000000100100000 | 2 | 1000000100100000 | 2 |
| 5 | 0010000000100100 | 2 | 0010000000100100 | 2 | 1001001000000000 | 4 | 1001001000000000 | 4 |
| 6 | 0010000000100100 | 3 | 0010000000100100 | 3 | 1000100100000000 | 4 | 1000100100000000 | 4 |
| 7 | 0010000001001000 | 3 | 0100000000010010 | 1 | 0010000001001000 | 3 | 0100000000010010 | 1 |
| 8 | 0010000010010000 | 3 | 0010000010010000 | 3 | 1000010010000000 | 4 | 1000010010000000 | 4 |
| 9 | 0010000100100000 | 3 | 0010000100100000 | 3 | 1001001000000001 | 1 | 1001001000000001 | 1 |
| 10 | 0010010010000000 | 4 | 0010010010000000 | 4 | 1000100100000001 | 1 | 1000100100000001 | 1 |
| 11 | 0010001001000000 | 4 | 0010001001000000 | 4 | 1000000010010000 | 3 | 1000000010010000 | 3 |
| 12 | 0010010010000001 | 1 | 0010010010000001 | 1 | 1000000010010000 | 2 | 1000000010010000 | 2 |
| 13 | 0010001001000001 | 1 | 0010001001000001 | 1 | 1000010010000001 | 1 | 1000010010000001 | 1 |
| 14 | 0010000001001001 | 1 | 0100000000100100 | 3 | 0010000001001001 | 1 | 0100000000100100 | 3 |
| 15 | 0010000100100001 | 1 | 0010000100100001 | 1 | 1000001001000001 | 1 | 1000001001000001 | 1 |

- a Data Frame,
- a Scrambled Frame,
- an ECC Block,
- a Recording Frame,
- a Physical Sector

# Error Detection

- Alphabet issues
  - Error → legal keyword
    - Detected at higher level of decoding
  - Error → illegal keyword
- Physical cause
  - Pit/gap edge shifted
  - Additional pit/gap



# Putting It Altogether

- Issuing: encode all $E = \bigcup_{i=1}^{3} e_i$ errors
  - Treat all detected $e_3$ like $e_2$
- Verification
  - **step I:** Verify signature
  - **step II:** Detect all $E_T = \bigcup_{i=1}^{3} e_{Ti}$ in-field
  - **step III:** Test $\left\| E \cap E_T \right\| \leq \alpha_T \left\| E \right\|$
  - **step IV:** Test $\left\| E_T \right\| \leq \left(1 + \alpha_X\right) \left\| E \right\|$

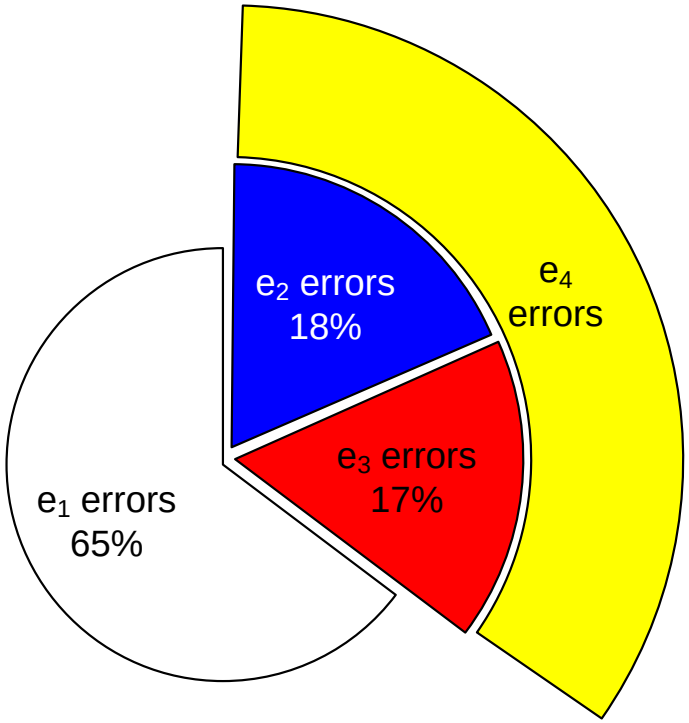
# Putting It Altogether

- False positives/negatives negligible
- Timing

Finally, we consider an implementation of o-DNA, where at an error rate of $10^{-3}$, an error read-out from the 24th millimeter (approx. $10^3$ revolutions) of a standard DVD-R disc, is sufficient to produce $||\mathbf{e1} \cup \mathbf{e2} \cup \mathbf{e3}||$ on the order of $10^2$. The resulting o-DNA message stored back onto the DVD would be approx. 1Kb long. Since the disc encounters 24 revolutions per second at 1x playback speed, one can observe that the verification of an o-DNA could be done in approx. $L$ seconds at 32x playback speed.

# Wear-and-Tear

- Due to aging, superior scratch resistance is required
  - Cost?




O. Slattery, et al. Stability Comparison of Recordable Optical Discs - A Study of Error Rates in Harsh Conditions. Journal of Research of the NIST, Vol.109, no.5, pp.517-524, 2004.

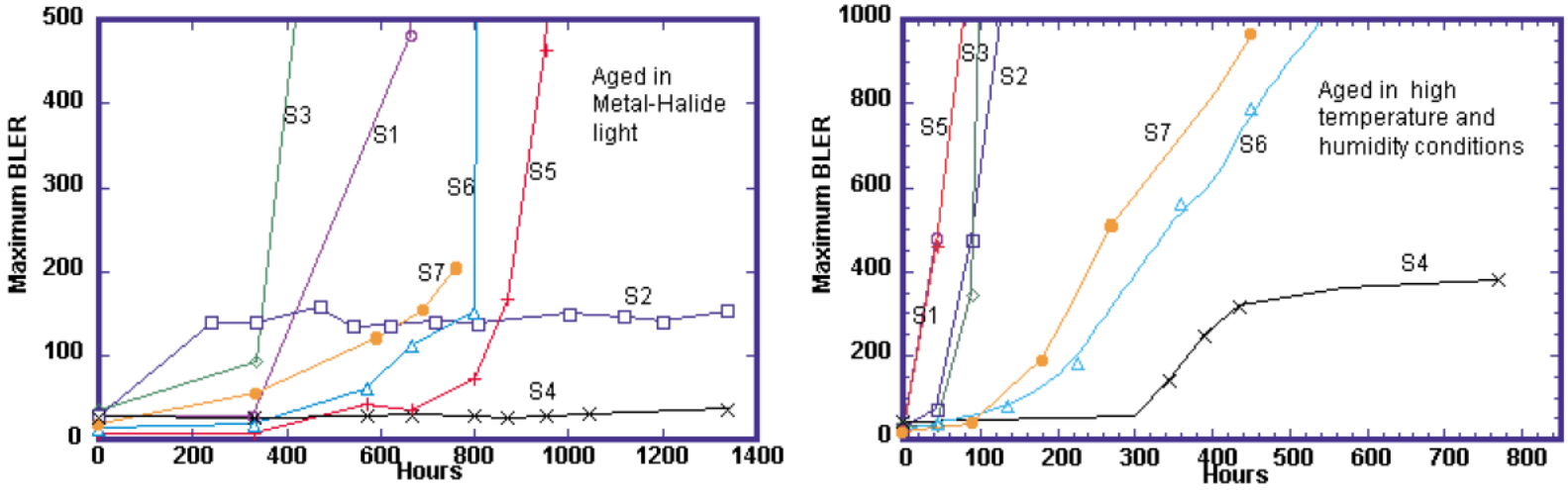



**Fig. 3.** Maximum BLER increase in CD-R when exposed to (A) M-H and (B) extreme temperature/humidity.

# Summary

- Anti-counterfeiting for optical media
- Cost = cents per disc
  - After a chunky initial investment, ~US$10M
  - Negative cost if you get rid of holograms
- False positives/negatives negligible
- Simple

# Acknowledgments


- Vencil Wells, **AudioDev**
- Dr. Holger Hoffman, **Technicolor**, USA
- **3DCD**, Technicolor, USA
- Dr. Paul Liao, **Panasonic USA Research**
- **Panasonic, Japan**
- Jared Feldner, **LeCroy**
- Hiroo Umeno and June Dorris, **XBOX**
- Gary Starkweather, David Heckerman, Yacov Yacobi, Jim Kajiya, Turner Whitted, Mike Sinclair, Gideon Yuval, Josh Benaloh, YuQun Chen, all **MSR**