PAPER

CRYPTOGRAPHY

Eric Rescorla, Stefan Savage, Hovav Shacham, Terence Spies
legal restriction
This dispenser is subject to restrictions on sale, modification, filling and use, and may be used only to dispense the trademark-bearing products identified on its exterior. Georgia-Pacific Corporation strictly prohibits unauthorized sale, modification, filling or use of this dispenser, and will enforce its rights under United States and foreign laws.

NEED ASSISTANCE?
Call Your Local G-P Distributor at:

or Georgia-Pacific TOLL FREE at
HELLO GP (1-866-435-5647)
“this dispenser is subject to restrictions . . . and may be used only to dispense the trademark-bearing products identified on its exterior”
problem:
“dryness theft”
and worse ...
largest company
making money
contributory dryness theft
2
solution?
use cryptography
cryptography

= 

business-model preservation
fathers
of cryptography
had in mind
“let’s give large companies the tools to screw over users”
Dryness
Rights
Management
chip on roll
pirates reuse empty roll
integrate with paper itself
encoded on roll:

\[
\text{roll id} \cdot \{ \text{Sig}_{SK} \left[ \text{roll id section } \#i \right] \}_i
\]
keep state to defend against replay
if verification fails?
degrade drying performance
and if pirates circumvent?
An Act

To amend title 17, United States Code, to implement the World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Digital Millennium Copyright Act”.
thanks!

creative commons attributions:
cleanwalmart, gehat @ flickr
Stefan Kühn, Poil @ Wikimedia Commons