


# PAPER CRYPTOGRAPHY


Eric Rescorla, Stefan Savage,  
Hovav Shacham, Terence Spies

< 1 >



*enMotion.*  
AUTOMATED TOUCHLESS DISPENSER

 Georgia-Pacific

Motion Activated 







enMotion  
WATER FILTERS





legal restriction



Model #

Date of Manufacture

FEB0707-A

C472004ZM



Georgia-Pacific

Commercial Products

## NOTICE

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)

GP4242-0670

property of Georgia-Pacific Corporation, Atlanta, Georgia.

leased to you for dispensing Georgia-Pacific products as supplied by an



“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 . . .



ADJUSTED VALUES  
\$7.97





largest company



making money

contributory  
dryness theft



< / 1 >



< 2 >



solution?

use cryptography



cryptology

=

business-model preservation

f a t h e r s  
o f c r y p t o g r a p h y



had in mind

“let’s give large companies  
the tools to screw over  
users”



Dryness  
Rights  
Management

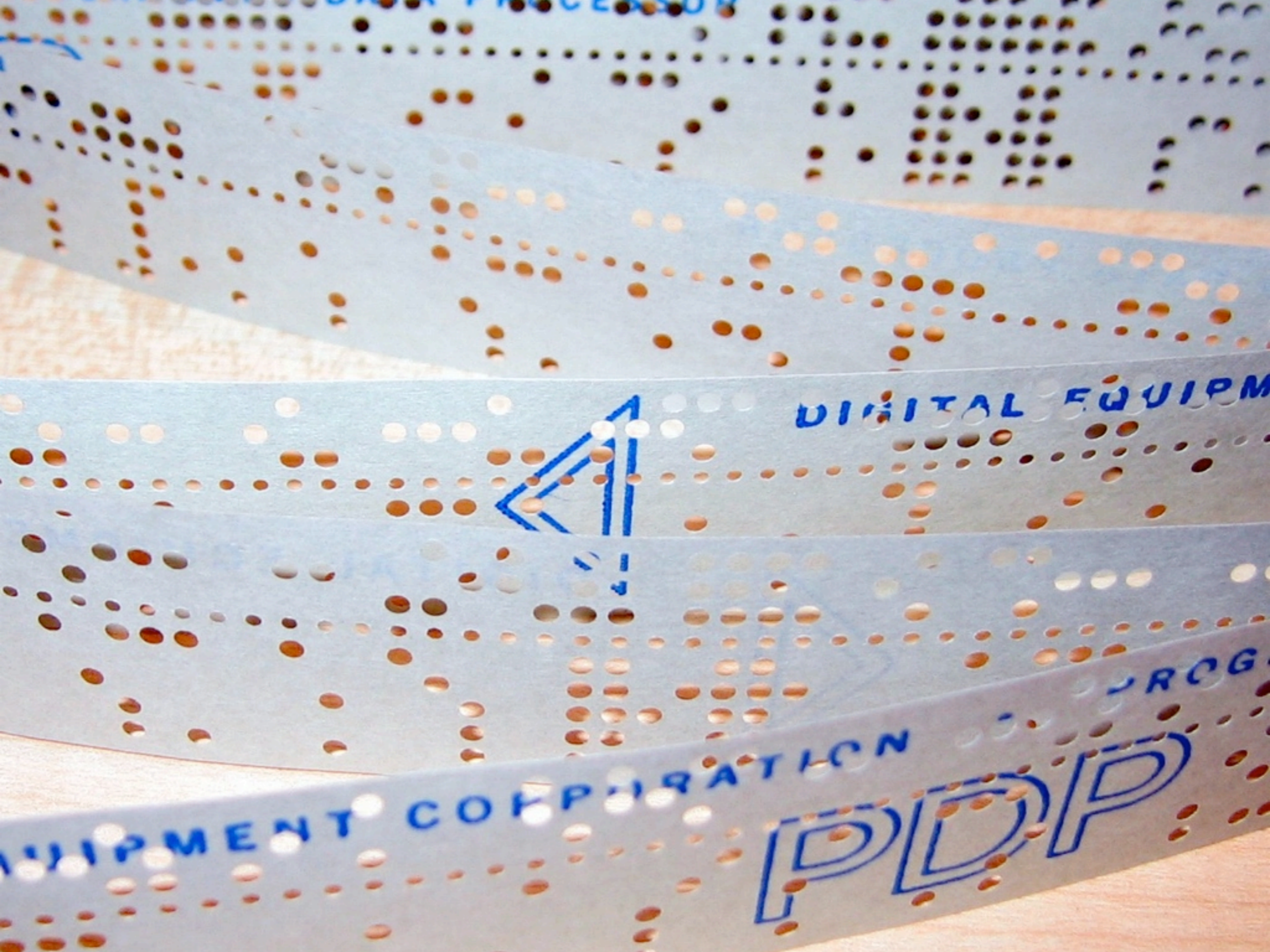
~~chip on roll~~



pirates reuse empty roll

integrate with  
paper itself



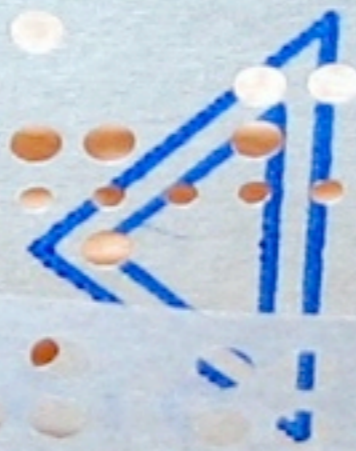


EQUIPMENT CORPORATION

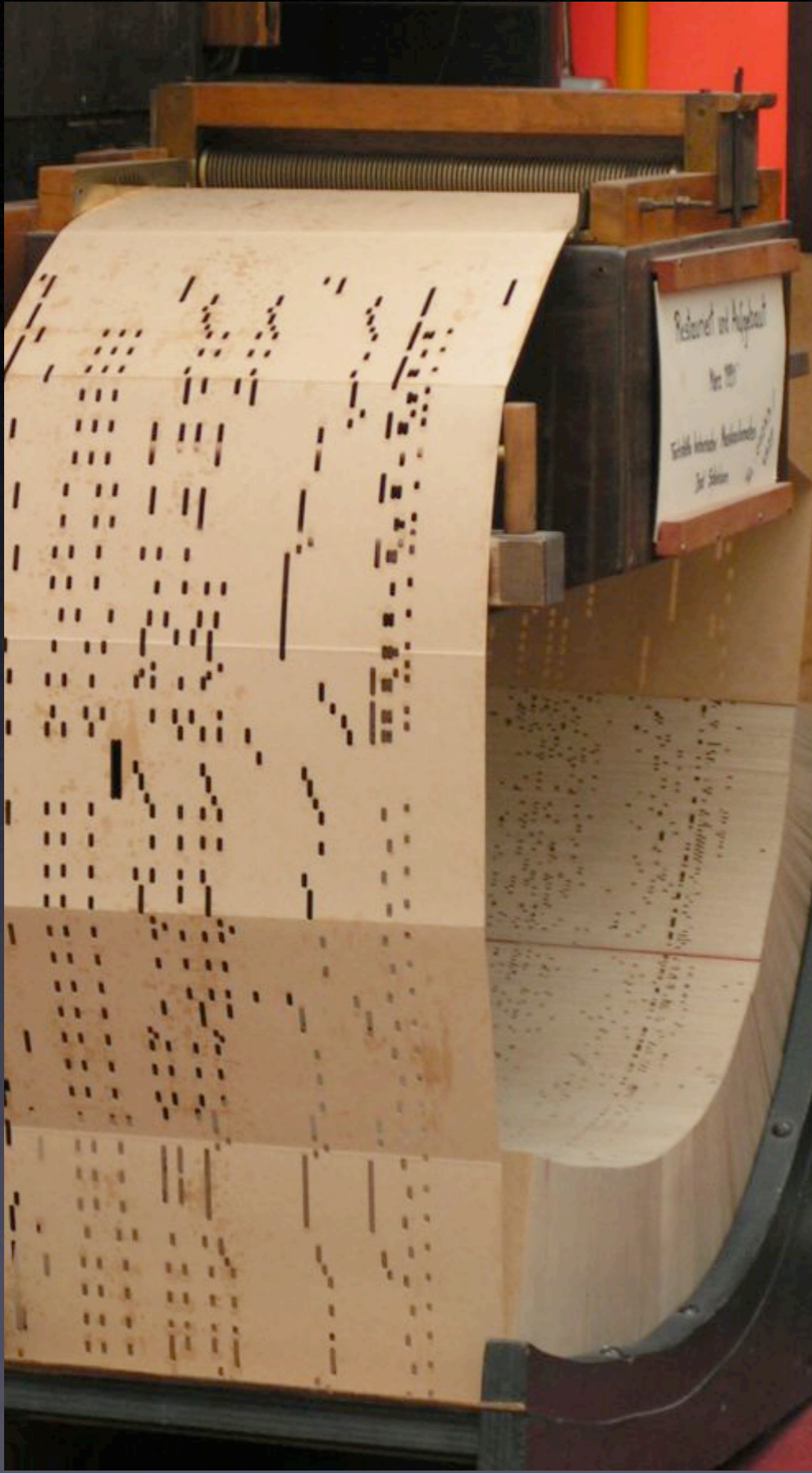
PDP

DIGITAL EQUIPM

PROG









encoded on roll:

roll id  
revocation block ,  $\left\{ \text{Sig}_{SK} \left[ \begin{array}{c} \text{roll id} \\ \text{section \#}i \end{array} \right] \right\}_i$

keep state to defend  
against replay



if verification fails?

degrade drying  
performance





< / 2 >



< 3 >

and if pirates  
circumvent?



One Hundred Fifth Congress  
of the  
United States of America

AT THE SECOND SESSION

*Begun and held at the City of Washington on Tuesday,  
the twenty-seventh day of January, one thousand nine hundred and ninety-eight*

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”.

< / 3 >



thanks!

creative commons attributions:

cleanwalmart, gehat @ flickr

Stefan Kühn, Poil @ Wikimedia Commons