Secure Deletion of Data from Magnetic and Solid-State Memory

Peter Gutmann
Department of Computer Science
University of Auckland

Secure Deletion of Data from Magnetic and Solid-State Memory

Peter Gutmann

Department of Computer Science
University of Auckland
`pgut001@cs.auckland.ac.nz`

Abstract

With the use of increasingly sophisticated encryption systems, an attacker wishing to gain access to sensitive data is forced to look elsewhere for information. One avenue of attack is the recovery of supposedly erased data from magnetic media or random-access memory. This paper covers some of the methods available to recover erased data and presents schemes to make this recovery significantly more difficult.

1. Introduction

Much research has gone into the design of highly secure encryption systems intended to protect sensitive information. However work on methods of securing (or at least safely deleting) the original plaintext form of the encrypted data against sophisticated new analysis techniques seems difficult to find. In the 1980's some work was done on the recovery of erased data from magnetic media [1] [2] [3], but to date the main source of information is government standards covering the destruction of data. There are two main problems with these official guidelines for sanitizing media. The first is that they are often somewhat old and may predate newer techniques for both recording data on the media and for recovering the recorded data. For example most of the current guidelines on sanitizing magnetic media predate the early-90's jump in recording densities, the adoption of sophisticated channel coding techniques such as PRML, the use of magnetic force microscopy for the analysis of magnetic media, and recent studies of certain properties of magnetic media recording such as the behaviour of erase bands. The second problem with official data destruction standards is that the information in them may be partially inaccurate in an attempt to fool opposing intelligence agencies (which is probably why a great many guidelines on sanitizing media are classified). By deliberately under-stating the requirements for media sanitization in publicly-available guides, intelligence agencies can preserve their information-gathering capabilities while at the same time protecting their own data using classified techniques.

This paper represents an attempt to analyse the problems inherent in trying to erase data from magnetic disk media and random-access memory without access to specialised equipment, and suggests methods for ensuring that the recovery of data from these media can be made as difficult as possible for an attacker.

2. Methods of Recovery for Data stored on Magnetic Media

Magnetic force microscopy (MFM) is a recent technique for imaging magnetization patterns with high resolution and minimal sample preparation. The technique is derived from scanning probe microscopy (SPM) and uses a sharp magnetic tip attached to a flexible cantilever placed close to the surface to be analysed, where it interacts with the stray field emanating from the sample. An image of the field at the surface is formed by moving the tip across the surface and measuring the force (or force gradient) as a function of position. The strength of the interaction is measured by monitoring the position of the cantilever using an optical interferometer or tunnelling sensor.

Magnetic force scanning tunneling microscopy (STM) is a more recent variant of this technique which uses a probe tip typically made by plating pure nickel onto a prepatterned surface, peeling the resulting thin film from the substrate it was plated onto and plating it with a thin layer of gold to minimise corrosion, and mounting it in a probe where it is placed at some small bias potential (typically a few tenths of a nanoamp at a few volts DC) so that electrons from the surface under test can tunnel across the gap to the probe tip (or vice

yl k y m yl j
l m
mg g m wy MFM
[4] [5]

O q w
yl mg m l
m w l m (w , w
gg /q g y l g
l mg mll
w l g l lg m x
q w q g ml
x q m I m ,
MFM m g
l mg m , q l l ml
, l y
m

E l yl x m
g g mg l
5 m g g l mg
l k q m g
k wl g k m , w ll-
m , l
l lg mg w l k
xm yl 2-10 m g kll
l q W
m x MFM l m
ll q yll l ll
mg k y g g MFM
ll w

, m m l g , l
SPM l y m
w l yl g k
l , m k k
l l g w l m
mg m yl SPM
w g mm l
ll yl w l w m
y I mm yl l l
SPM x , l
l yl l SPM US$1400,
g PC ll [6]

F w q MFM, yl l g
m mg m y l
lm l w w
m m, w l y m ,
l, mg m yll
l y w g w x yl
m l m, yll

m y l g
m m g

I l m, w w k
m , w z w
m z Hw l
l g 0 95 w z w
w , 15w w w
N m l k y
l , g l y
l w k w 'l y ”
y l w ly
w ’ m y g
g l m lg l w
gq l y g l ml g ll ,
w l g ml w m PC,
yl g w yl
g l W w g
“ ”l g l m w w
yll , l g m
g l S lg y
mm l w q l y
y ll ml
g ,l l y x l x
m w ’ xl y
l (l g w w l g
q RL (xl w
q x m g l g
ml l ll yl
l g l

U g MFM, w g D g
ml k l g
g l k y m mg z
k g myl m l
g l g l ml g
g yl m
mg z k g ,
w w ll w
w l
q MFM S M (
“ ”l MFM S M l
k - g
m m [7] M l
m g l g
y (y l y
g g k w l g yl
g l w w
y g g y w
k, w g m w l
- k m g l
m k mk g g g k
l l (

m g l y m y l
y x lm

l q l l w
m mg m l g
w l g
y g l F x m l x m AC
l g w w 40 MHz
q w w l 12 mA w
w 2 mA 1 1 1 2 mA
, mg m
lw w g m g m m
lwmll m Ay m l y
g w y
, l ll gMM

E w DC ,
yl g lmy l l
DC l l m m yl

D m
g l k my l g
l g k g l yl
N wly w , w
l g lg k MFM S M
mg , m yl
w k g
Rg w l w
mg z w w Hw ,
w w
, w m *erase band* w
mg z j l
w k w l
y m w l g
mg z , mg
g g w wll
O x m l w g x l
l w l 25 nm g w
- k y xm yl l k w ,
w g g w q y l g y
g yl k
l 2.45 µm ll l
w l w
k U g 42 µm w
xm yl l µm w w l
w k w 180°, g nh
g w w k w - W g
g q y w g l k
l 0.5 µm w k l
0.49 µm llw lg MFM mg l
l , w g m
w w
k m m -

I , w k w x
m l w l
w l w , l w g
l
m l l g
w m l
w l g yl w k
I yl lg w k w
m l yl g ; m
k m m k y
m m g l k
l g w yly g l l
l w q y
g l w

W ll m
k mg y g
w , m
ly " g g yl mll k
w m I llg g *lot*
x g lm mg

3. Erasure of Data stored on Magnetic Media

g l w g m
l mg m k k
m l (
g g w w g m w
w I w yl w l
myl w
z w yl Hw , k
g yl m m l- g lm (RLL
g j w ' w
g ,
l l y g , , w
w l m w l l k w w

mg m ,w w m y
m w l g x
mg l ll g g
l g mg m
l m m U yl
ml w k
g l, y g
q y g l y " "
mg m m D k m , y g
- g , g
l q , w w yl q
lw q y k E
ll g w

lw q y l w ,
yl l gm m
w q y l m w yl
w
l mg w g
l g m l l m
y l k w
20 B w m w
40 kFCI (1x g , y l
k , w w g l y g
m 0 100 kFCI g m
w w
g l 10 kFCI, w w m
g 100 kFCI [12] k w w l
y w q y — q y
, w w MR
EF I [13] w w w
20% w q y w
m l 40 kFCI, w g m
m k g q y g
Hw , w w l y
g w -
m w m yl w
q y q l DC w
m y l w
w , w w g
y (xl
- g y w , g -
y

y w lw l q y w m
m w w l w-
q y g l

I y
w , y k
l k g m k
m lm g y
y , k lg g l
m w m y
m l , g ym l
w l l
k l y l y
ym l y g
wy lg g l k
l y yl
k (yl l yl
transitions mg , ml g
l
0
/g k l g (
m “ k ”l
, w l k

z g S l g g 0 wl mk
l k g l, w lm
m x m m m 0
k mlm m m l- g -
lm , EL, g

RLL g m
y l- g lm (*d*, *k* , w *d*
m mm m 0 ym l w m
w l ym l ,
k mxmm m (*d*, *k*
l j l g lm
w ym l ,
w l y

g ll RLL w FM, w
w llw y l k ,
l w w (l
w l g w l 0 w
(½ w l g A w
k m FM (MFM , w
l k x w j 0 (m g y
m MFM F m
wl m FM
mg m y k g x m l
q 0000, 1111, 1010, wl
0(1 0(1 0(1 0, 1(0 1(0 1(0 1,
1(0 0(0 1(0 0 w (l k
y g m x m m m
w l w 0 (k
m m ,
wy l 0 (k
lg g l l w m
, l g (3 RLL (3 RLL/MFM
l ll g l y y
yl l y w m
kw - m l

l ym l ,
k
g y m
w k
g y MFM w g yl l y
2, EL (g 1EC m ,
y (1,7 RLL, w l l
g l

U g k wl g w , w
w w w
g l
g m
mj y mg k Hw ,
l l W MFM, y

w y q y w (1,7 RLL l l z F MFM w m m w , lw w q y l y w g g 1010 0101 l y “ ” , g “1 K” ll 0 W w l l lk w y l k l l 0 l MFM g (“ l ” g l m k k y w m w , w g y g 100100, 010010 001001 W l l w , MFM l , lw - y (yll y w y l y A , y m w m q m w k m w m

F m MFM w j m x ml , w (1,7 RLL A g m y 8 m w , lw q y w 6 m w l y m w l k y y ll (1,7 RLL m y W w wy w w k w g l (1,7 RLL W y l k g wy - y m w k - l , g g yl I m k w k w l g l lm ml , l y m l m

D y y , g w l g g 6 l g S 2/3, g 4 y 16 l , m k g l w ll m g S g w g (1,7 RLL k, w w 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111 l yl w MFM w , l g w l w m

MFM g

F y w (2,7 RLL ml MFM g - - m g l w m , ll A x - m g l w l ll m g k U g ½ g , g - - m g l g 4 m mm (2,7 RLL w 1 1

Decoded Data	(2,7) RLL Encoded Data
00	1000
01	0100
100	001000
101	100100
111	000100
1100	00001000
1101	00100100

1 1: m mm 2,7 RLL C

m mm (2,7 RLL m w “ ” m l m , w ’ l W g q y g 0x33, 0x66, 0xCC 0x99, w l y w 2,7 RLL

Sx - m w g 3 g -l -l l w 2,7 RLL , l g x :

```
001001001001001001001001
   2   4   9   2   4   9
```

y 0x24 0x92 0x49, 0x92 0x49 0x24 0x49 0x24 0x92 x

```
011011011011011011011011
   6   D   B   6   D   B
```

y 0x6D 0xB6 0xDB, 0xB6 0xDB 0x6D 0xDB 0x6D 0xB6 x m MFM , w y x 2,7 RLL

A g (2,7 m l (-1990) , m l ll (2,7 RLL, w - g l l y w lkl y w l m m m m, g w m m l y lm w , w w ’ w , w l

m m d v v m b m
b - d w b w m b
b w d .)

T d- d v m d P -
R p x m rh d RR L) d
w m b q d d
d b V.32 m d m v b
rp p v . RR L d RLL
d b w mw d . A
p d m v 0 4 4 w
0 m 1 d m
x 0 p d
p d 4 m b
m 0 b w 1 d m
d d 4 p m x m m rh 0
b w 1 rh b q . PR L
d v d rh b
d q p d
x b d d q d m
p " p " p RR L) wd
b m x m m d d d d
d m m q d b
w w d "m x m m
dp RR L)

RR L v m w b
d d p d- m d b w m
d d w m d
d m d . Sv m
d mv p d b d p d
RR L v 30-40% d
v d d RR L 4

S RR L d d ' p p
m w RR L RLL d d w d
w v dm p b
p d d v rp x d
. F d v p m
m md m m d d v v d d
b d d w m m m
dm p p
m md PR L
d v d d 6700 P
p) d d d d 170 E
d b 1 7 RLL q v .
A v d- v d
d w m p
w d v p
d w d d b m
b d [15]. S w m d
m b d p d
v b d .) d v q

p d p j d m
w d d v w
p d m d . A d b w
dmd w d b w b p d

W w v 2 v w p w
d v d w
d . T b d b rp v d
b d dm p b d
p d b p m d m
p dm d m m d
w w d p w md
w p . T d w v w
p w q 3 v w
w Tb 2

T F-p p p d w b
F d v v w d d
p x m . T d m
p b w dm w p m d
b w p md m m d
p w d d
w rp v v w d
w d p p dm
rh p m p m v d
p b m p w d
v w p b b p d p v p
d " " p b b w
v w d .)

dv b w p
b d d b d b d
p d w p md p
d v b p b
b . F x rp p d b
d d SCSI-2 G p 1 w mm d b
F U A b SCSI mm d
b pp d v b
w w b d w b
— m rh v w m b
dp .) A d w d
b w d
w d v m m
- v p v SCSI
d d v p mm d
m w v w
m SCSI p .) T m
d v FORMAT UNIT mm d m
md w p m m
rp p m d d m
mm p) m w d d
SCSI-2 d d d z p
P p FORMAT UNIT mm d

wv **p** d b x d d b b b d v) d d m **p** d b m b w — b w q m — d d v v d d **p** d v v d .) b b d d b mv md m

Pass No.	Data Written	Encoding Scheme Targeted
1	R d m	
2	R d m	
3	R d m	
4	R d m	
5	`01010101 01010101 01010101 0x55`	1 7) RLL F
6	`10101010 10101010 10101010 0xAA`	1 7) RLL F
7	`10010010 01001001 00100100 0x92 0x49 0x24`	2 7) RLL F
8	`01001001 00100100 10010010 0x49 0x24 0x92`	2 7) RLL F
9	`00100100 10010010 01001001 0x24 0x92 0x49`	2 7) RLL F
10	`00000000 00000000 00000000 0x00`	1 7) RLL 2 7) RLL
11	`00010001 00010001 00010001 0x11`	1 7) RLL
12	`00100010 00100010 00100010 0x22`	1 7) RLL
13	`00110011 00110011 00110011 0x33`	1 7) RLL 2 7) RLL
14	`01000100 01000100 01000100 0x44`	1 7) RLL
15	`01010101 01010101 01010101 0x55`	1 7) RLL F
16	`01100110 01100110 01100110 0x66`	1 7) RLL 2 7) RLL
17	`01110111 01110111 01110111 0x77`	1 7) RLL
18	`10001000 10001000 10001000 0x88`	1 7) RLL
19	`10011001 10011001 10011001 0x99`	1 7) RLL 2 7) RLL
20	`10101010 10101010 10101010 0xAA`	1 7) RLL F
21	`10111011 10111011 10111011 0xBB`	1 7) RLL
22	`11001100 11001100 11001100 0xCC`	1 7) RLL 2 7) RLL
23	`11011101 11011101 11011101 0xDD`	1 7) RLL
24	`11101110 11101110 11101110 0xEE`	1 7) RLL
25	`11111111 11111111 11111111 0xFF`	1 7) RLL 2 7) RLL
26	`10010010 01001001 00100100 0x92 0x49 0x24`	2 7) RLL F
27	`01001001 00100100 10010010 0x49 0x24 0x92`	2 7) RLL F
28	`00100100 10010010 01001001 0x24 0x92 0x49`	2 7) RLL F
29	`01101101 10110110 11011011 0x6D 0xB6 0xDB`	2 7) RLL
30	`10110110 11011011 01101101 0xB6 0xDB 0x6D`	2 7) RLL
31	`11011011 01101101 10110110 0xDB 0x6D 0xB6`	2 7) RLL
32	R d m	
33	R d m	
34	R d m	
35	R d m	

Tb 2:O w D

4. Other Methods of Erasing Magnetic Media

T p v d m d w q p d q pm p m . A v m md w d q p d q pm d p w d md d) d p d . D b v m p d m m d md d w v w m d v w m m m d d v d db b 2d .J

T w dm m p m m z d q v m b w x m d p w b . T w dp d m d x d b m w p d F p d d v md - m d dd p m dm b d b ⅓ v md x v w d md p)I

Hwv v md m x v d m b m m q m b v m v md m [8] v m x m d p m p d d p w DC d p w m 1 Hz). C v m d O d O) p p m m d d d m m d d m d m z — v d d m md m Tp v p m md v Tb 3b w

Medium	Coercivity
5¼" 360K pp d	300 O
5¼" 1.2 pp d	675 O
3" 720K pp d	300 O
3" 1.44 pp d	700 O
3" 2.88 pp d	750 O
3.2 p d	750 O
O d 19) d d	900-1400 O
N w 19) d d	1400-2200 O
1 m p	300 O
¼" Q C p	550 O
8mm p p	1500 O
DAT m p p	1500 O

Tb 3: Tp d C v F

US Gv m d p 350 O v w C p d p 350-750 O v - C p . D v b b p p . Tp v 750 O v d C w w d pb m b w [9] v m pw m AC d mm dd 7 500 O dd p DAT p d d b p.

D d md mw m d — v d d d v v q v C p m m d . S m d p d m d w m b p md m b d d d d b d b w d w m m mp b v m b p d md mp d d b D d m d p p dd d md d d v b m d p m q v p d .) d p d q p d q pm w p v d d b x mp dq d w 2.5 W Nv m d b m P m d ¼" d d v 1½ m . b p d v d p bb dd b d pb d v mp [9]

5. Further Problems with Magnetic Media

A mj w b d d
d d w b- d v w q
p b m d v d . W d v
m d d d
w dd d d w m p
d d w d d
d v dd d d b d v
b d v m m w . T v
q w d m d
d . T mv d m
w d w d . T m
pp b
d m w d q
d d w
w d p d d
p m d w d
b b
p . A m b p d
m d m m m
m

A d q
d m m
d b d v . T m
d b m v d d
. d d b
p b 9%

A d q p
p d b q
D p d v d d
p d
p p d v w d
d . T d w
b m p d v
[4]

T d m pp d d
w ' b vd w
p d d v m . A
m SCS d IDE d d v m w
d d v m pp d m b
d m - d d v-p
m . F xmp SCS -2 READ DEFECT
DATA mm d b d b
d v d v. S SCS b
rh m b m pp d b
d d dd m d
d . A SCS dv d
p md m b rh m pp d-
b d d T
b p b p b v
m vd
v md p SCS dv p
vd d p
mp d v . T
READ LONG d WRITE LONG mm d
w w d x d v
p vd) p m
p d v d
REASSIGN LOCKS mm d
d v . Hwv p q
dp w d p SCS
dv d x v d d v d m
d p p v
p p .

T ANS X3T-10 d X3T-13 b mm
w d d
U v S R m mm d IDE d
SCS d d w w d . T
w v v m p p v w p w
v m pp d d w d b -
w . d v v b d b md d
mv p d d
w mv p p d
d d b d v m
w m b d d
mm dw b p .

L - m v m d
b m md . F xmp m
p m p b m d
b d v d mp
v d m m z p
d b p d m [22]. T m p
m d md w d b
v d b dd [23]. T b
d dp d m m b d
md md
xmp v- - d w d
b w w d .)

T dp d md v mp
v w pb d w
dd mp w v w w
dd p p d d p
md) b m b v w mp w
v v . T mp
d d d v w mp v
dp d w b d d
d v w pw - v b d
w d q b d Hwv
v w p m dp d
mp dp d md b
mp dp d vd

d T rh m mm md d d v w v mm p vd d p d v w p m w d d d b p d v rp -40°C +40 d rp m d 4

A w d b b m w dv v m v m b m dm d m v - m . A d b d m p b- m d p d - d ECC) pb m p b . A p d v m v 2 b d 4 b CRC d 1 b ECC p . T ECC w d b pb b p 2 b d b b p 1 b d d b p 5 b b p 1 b [25]. A d v m q b p 120 b p 32 b 18 b R S m ECC [26]. T v m d b d m b p b v b - - pb d v . C v m w m d ECC m x rp SCS - 2 WRITE LONG mm d w b d w d d m d) d m d v b .

6. Sidestepping the Problem

T w v p b m v m m m md v md p . A p d w w p p p rp m p m v b w d . T w d p p w mm p d d b p m w b v d d m w w w mm d m d m wp x rp x w w w W d w wp m DOS p p m) A v w w d p d v w w w p m m b b v m x rp x w w w m d v NFS w d b md d w m m d p mv d m w d w p d [27].

T v p b m mm p m b d p v m m b p d d m d v w . T p b p b w m d p d mm b v b pq d d p mm p v d d d OS w) p v m b p d [28]. T x d p mm dp d p m b d U x m w p `mlock()/munlock()` v m v m m d m `mmap()` - d w b d p mm . U p q p p v d b p rp m p m mm d O m W d w NT w p mm w `VirtualLock()/VirtualUnlock()` b m rh w b d

p m v v v mm d d v d p p m p v b) mv p " " w mm d T m p mm m mm w z w md b p m . T v d p d p m d d rp m v mm . U x m v b p p m p w p m b d b p m. A m rh p m p p m p w p d m xd d m v b) rh p m d p p b . T m m m m v p v d p d) rh p v b p . O d m m w v p rh p . T m v d b w w d p m p p m xd rh p w

m y m
k m y ma my
y .

I m
y m. A y
m m v y m y
v y y m y
mm y y y m
y m k z 1K
mm y (m y y m
m m
m y)
m v y y ma
m . O m k
v m
(xm HTTP v SSL)
k m my m
.

7. Methods of Recovery for Data stored in Random-Access Memory

C y v m “v ”
m mm y y
mv . B (SRAM)
y m (DRAM) mm y m
m
. SRAM y
m m v
m
-
mv . O SRAM
“ mm ” v y v y.
I m SRAM
y v -
v — k “ ROM
DRAM “ mm ”
y y I ’ m
(v
) y RAM
x m
y y
y x
y . O
RAM
m ()
m
m
y m y
m v . H v v x j
v y .
W m m m m
mm — v y v y
y m (m) m
v . I
m v v y
m
m x q y m
x m . I
z v m
v .y

T m v m k
PC . I y
m v y “ ”
q (v y k)
. T RAM
m -
v y m
k v m
m . C m
m x . M y
DRAM v m m
m m IO m y
RAM m v. T
m y y v y RAM
m y
y m v v m .
M ’ m
y ’ m
m y j v m y
v m y
.

A m m v m
m
mm y . B DRAM SRAM
m q ky $T_{junction}$ =
140°C y m m . Sv
m
y mk v y
. C v y x
mv m
-60°C. S
k y .

8. Erasure of Data stored in Random-Access Memory

Sm y y v DRAM
’ y v

m m . T
x x
x mm y k “ ”
v “ ” k .
T m m
x m “ ”
m x .
G y
x m m . T
m
y v v
x . I y x x m
m
“ ”
. U y
m x y RAM

T m mm y

y . C v y
m
“ mm ” y
. B DRAM m
m
y ’ . O
m y 0 m
y .

T m m DRAM
y
mm y mm y v
“ mm ”. W

m m vy v y
ky. T y v ky
m mm y
m m
m ky
y k v. T -
v - k
y ky q
m y y m m m y
k m
.

9. Conclusion

D v my v y
x m
m y . D
v y m m
v v ’
m (

m m) vy m
y
(RAM). F vy m
y m v
m m m y v m
. H v y
vy m m
k k m y m
vy x v.

Acknowledgments

T k k N B P
F k A y H Kv M z C
P m C P v
.

References

[1] Em y D I m S M ” MS zk I D A y D m 97

[2] “A G U D Rm A m I m S m” N Cm S yC S m 9

[3] D D I m m E M D k” V V v M C M U v y 8

[4] M m y G m ” R MM m G S m SJ M F y Y *Journal of Applied Physics* **Vol.68 No.3** (A 1990) .1169.

[5] T - z M F M y B T k H D k P R J M *IEEE Trans.on Magnetics* **Vol.27 No.3** (M y 1991) 3452

[6] N T : T Hm STM P ” J m R `http://www.skypoint.com/-members/jrice/STMWebPage.html`.

[7] M F S T M h O D ” Rm Gmz An A y I k My y E B k *IEEE Trans.on Magnetics* **Vol.28 No.5** (S m 1992) 3411

“Comparison of Magnetic Fields of Thin-Film Heads and Their Corresponding Patterns Using Magnetic Force Microscopy”, Paul Rice, Bill Hallett, and John Moreland, *IEEE Trans.on Magnetics*, **Vol.30**, **No.6** (November 1994), p.424 .

9 “Computation of Magnetic Fields in Hysteretic Media”, Amr Adly, Isaak Mayergoyz, Edward Burke, *IEEE Trans.on Magnetics*, **Vol.29**, **No.6** (November 1993), p.23 0.

0 “Magnetic Force Microscopy Study of Edge Overwrite Characteristics in Thin Film Media”, Jian-Gang Zhu, Yansheng Luo, and Juren Ding, *IEEE Trans.on Magnetics*, **Vol.30**, **No.6** (November 1994), p.4242.

1 “Microscopic Investigations of Overwritten Data”, Romel Gomez, Edward Burke, Amr Adly, Isaak Mayergoyz, J.Gorczyca, *Journal of Applied Physics*, **Vol.73**, **No.10** (May 1993), p.6001.

2 “Relationship between Overwrite and Transition Shift in Perpendicular Magnetic Recording”, Hiroaki Muraoka, Satoshi Ohki, and Yoshihisa Nakamura, *IEEE Trans.on Magnetics*, **Vol.30**, **No.6** (November 1994), p.4272.

3 “Effects of Current and Frequency on Write, Read, and Erase Widths for Thin-Film Inductive and Magnetoresistive Heads”, Tsann Lin, Jodie Christner, Terry Mitchell, Jing-Sheng Gau, and Peter George, *IEEE Trans.on Magnetics*, **Vol.25**, **No.1** (January 19 9), p.710.

4 “PRML Read Channels: Bringing Higher Densities and Performance to New-Generation Hard Drives”, Quantum Corporation, 1995.

5 “Density and Phase Dependence of Edge Erase Band in MR/Thin Film Head Recording”, Yansheng Luo, Terence Lam, Jian-Gang Zhu, *IEEE Trans.on Magnetics*, **Vol.31**, **No.6** (November 1995), p.3105.

6 “A Guide to Understanding Data Remanence in Automated Information Systems”, National Computer Security Centre, September 1991.

7 “Time-dependant Magnetic Phenomena and Particle-size Effects in Recording Media”, *IEEE Trans.on Magnetics*, **Vol.26**, **No.1** (January 1990), p.193.

1 “The Data Dilemna”, Charles Preston, *Security Management Journal*, February 1995.

9 “Magnetic Tape Degausser”, NSA/CSS Specification L14-4-A, 31 October 19 5.

0 “How many times erased does DoD want?”, David Hayes, posting to `comp.periphs.scsi` newsgroup, 24 July 1991, message-ID `1991Jul24.050701.16005@sulaco.lonestar.org`.

1 “The Changing Nature of Disk Controllers”, Andrew Hospodor and Albert Hoagland, *Proceedings of the IEEE*, **Vol.81**, **No.4** (April 1993), p.5 6.

2 “Annealing Study of the Erasability of High Energy Tapes”, L.Lekawat, G.Spratt, and M.Kryder, *IEEE Trans.on Magnetics*, **Vol.29**, **No.6** (November 1993), p.362 .

3 “The Effect of Aging on Erasure in Particulate Disk Media”, K.Mountfield and M.Kryder, *IEEE Trans.on Magnetics*, **Vol.25**, **No 5** (September 19 9), p.363 .

4 “Overwrite Temperature Dependence for Magnetic Recording”, Takayuki Takeda, Katsumichi Tagami, and Takaaki Watanabe, *Journal of Applied Physics*, **Vol.63**, **No.8** (April 19), p.343 .

5 Conner 3.5" hard drive data sheets, 1994, 1995.

6 “Technology and Time-to-Market: The Two Go Hand-in-Hand”, Quantum Corporation, 1995.

7 “Basic Flaws in Internet Security and Commerce”, Paul Gauthier, posting to `comp.security.unix` newsgroup, 9 October 1995, message-ID `gauthier.813274073@espresso.cs.berkeley.edu`.

2 “cryptlib Free Encryption Library”, Peter Gutmann, `http://www.cs.auckland.ac.nz/~pgut001/cryptlib.html`.