

SR/CL: MAY DAY, 1998

LEITMOTIV: "The material world exists nowhere but in the mind." — Jonathan Edwards

$$\hat{T} = -i\hat{\alpha}_1\hat{\alpha}_3\hat{K} = i\gamma^1\gamma^3\hat{K} = \hat{T}_0\hat{K}$$



Luther
9,192,631,770 Hz

"I am Your passing guest"
—Psalm 39:12
 $[x \mapsto (X \rightarrow X_{xy})]$

"History is a pattern of
timeless moments."
 $|T\phi Z| = 3$; —Eliot

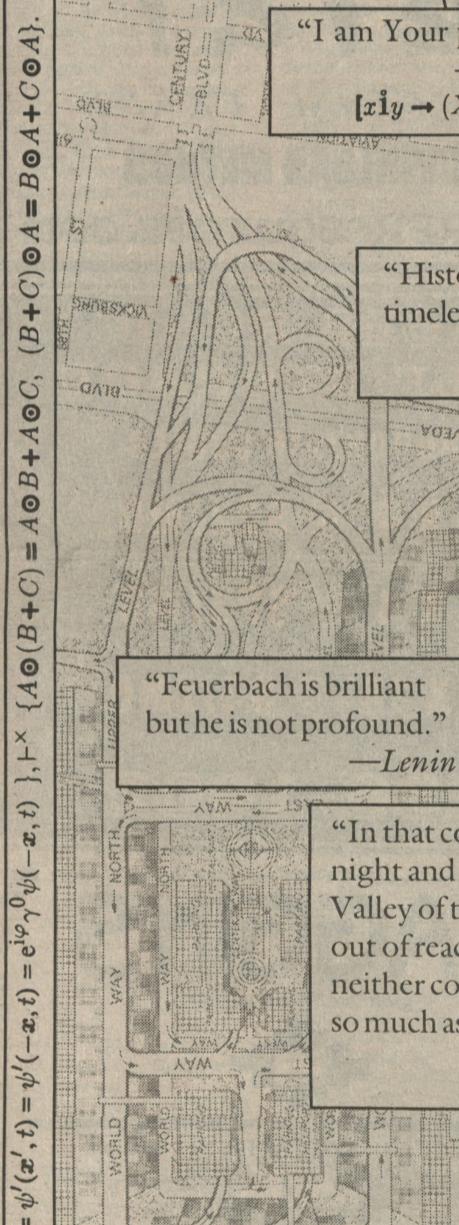
"Feuerbach is brilliant
but he is not profound."
—Lenin

"In that country the sun shines
night and day, for it is beyond the
Valley of the Shadow of Death and
out of reach of the Giant Despair;
neither could they from that place
so much as see Doubting Castle."
—Bunyan

$$H(Z[y/x]) = xFz$$

"When that Arcite to Thebes comen was,
Ful ofte a day he swelte and seyde 'allas,'
For seen his lady shal he never-mo."

—Chaucer, *The Knight's Tale*
 $\Theta_3 \emptyset \neq \Theta_3 \cap \Sigma_3$



typedef s
unsigned

} a5-ctx; ADW, 5/1/93@***(**)

static int threshold(r1, r2, r3)

unsigned int r1>ADW 5/1/88#3cf/

total - (((r>> 9) & 0x1)==1)+

*ADW 5/1/92***

clock; ADW 5/1/89;

3456789 ABC...Z(1)

*phertext: cab920cd d66144138

6789ab def01234

Block%decrypts

printvec("CIPH")

ec ("PLAIN="

intvec<IFF>c

not in ECBm

lock (*11697)<GtWbRe/1

ΕΞΑΓΟΡΑΖΟΜΕΝΟΙ ΤΟΝ ΚΑΙΠΟΝ

Digital signcryption or how to

achieve cost(signature & encrypt)

ion). In Burton S.

Kaliski Jr., editor, *Advances in C*

Computer Science

, pages 165-170. Springer-

Verlag, 1997. [BibTeX entry]

Rohit Sethi, "A Cryptanalytic

Attack on the McEliece Public Key

Cryptosystem," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 August 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus

tom 1997. Springer-Verlag. [BibTeX entry]

Thomas A. Berson, "Failure of the McEliece public-key cryptosystem under message-reser

ved related-message attack," In Burton S. Kaliski Jr., editor, *Advances in Cryptology - C*

RYPTO '97

, volume 1294 of *Lecture Notes in Computer Science*, pages 213-220, 17-21 Augus