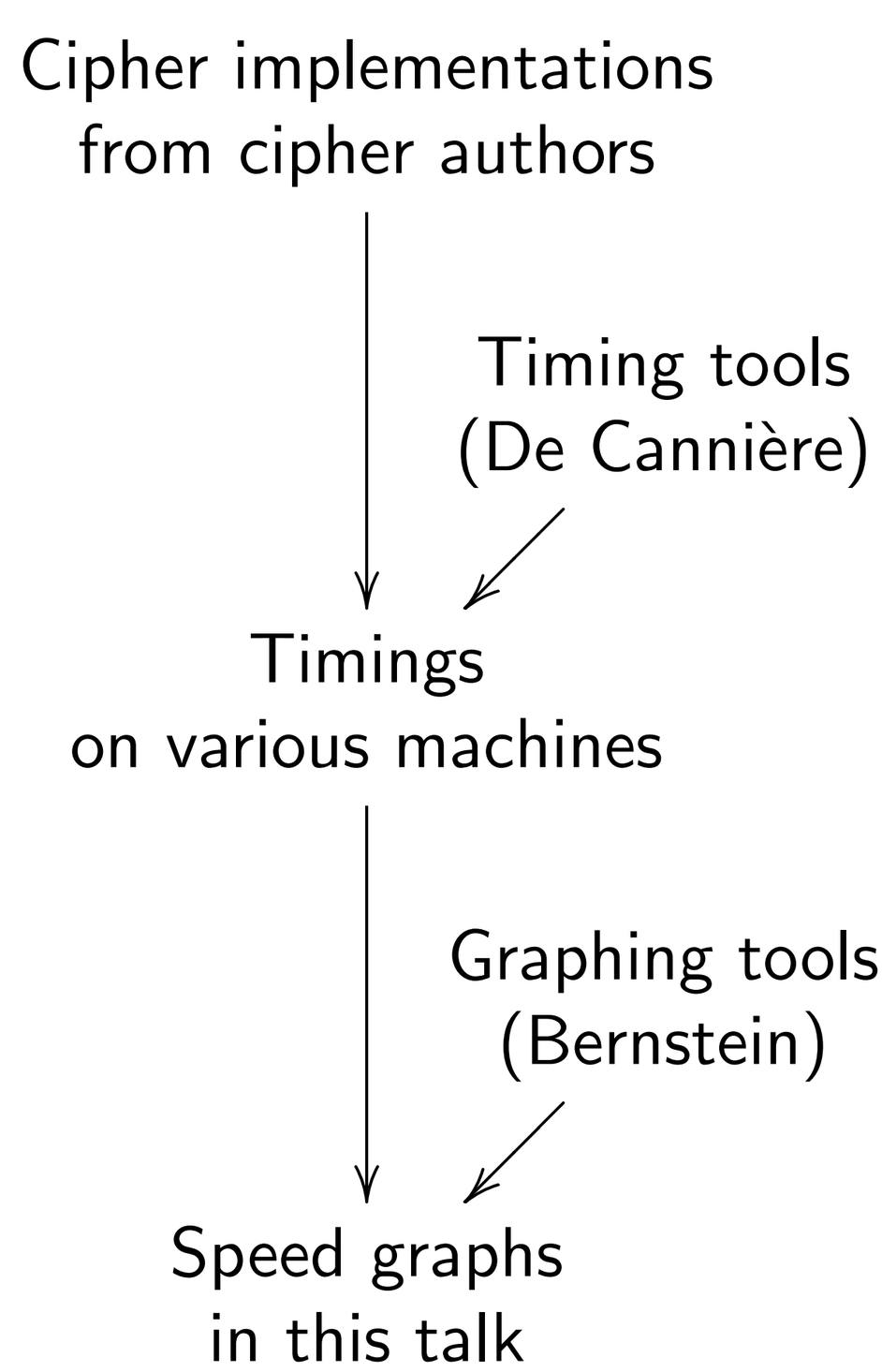
Comparison of
256-bit stream ciphers

D. J. Bernstein

Thanks to:
University of Illinois at Chicago
Denmark Technical University
Alfred P. Sloan Foundation



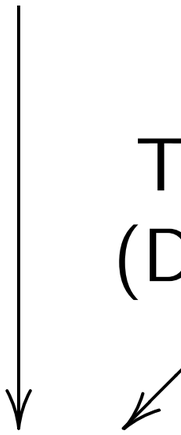
phers

pis at Chicago

al University

oundation

Cipher implementations
from cipher authors



Timing tools
(De Cannière)

Timings
on various machines

Graphing tools
(Bernstein)

Speed graphs
in this talk

Security disasters

Attack claimed o

Attack claimed o

Presumably also

Attack claimed o

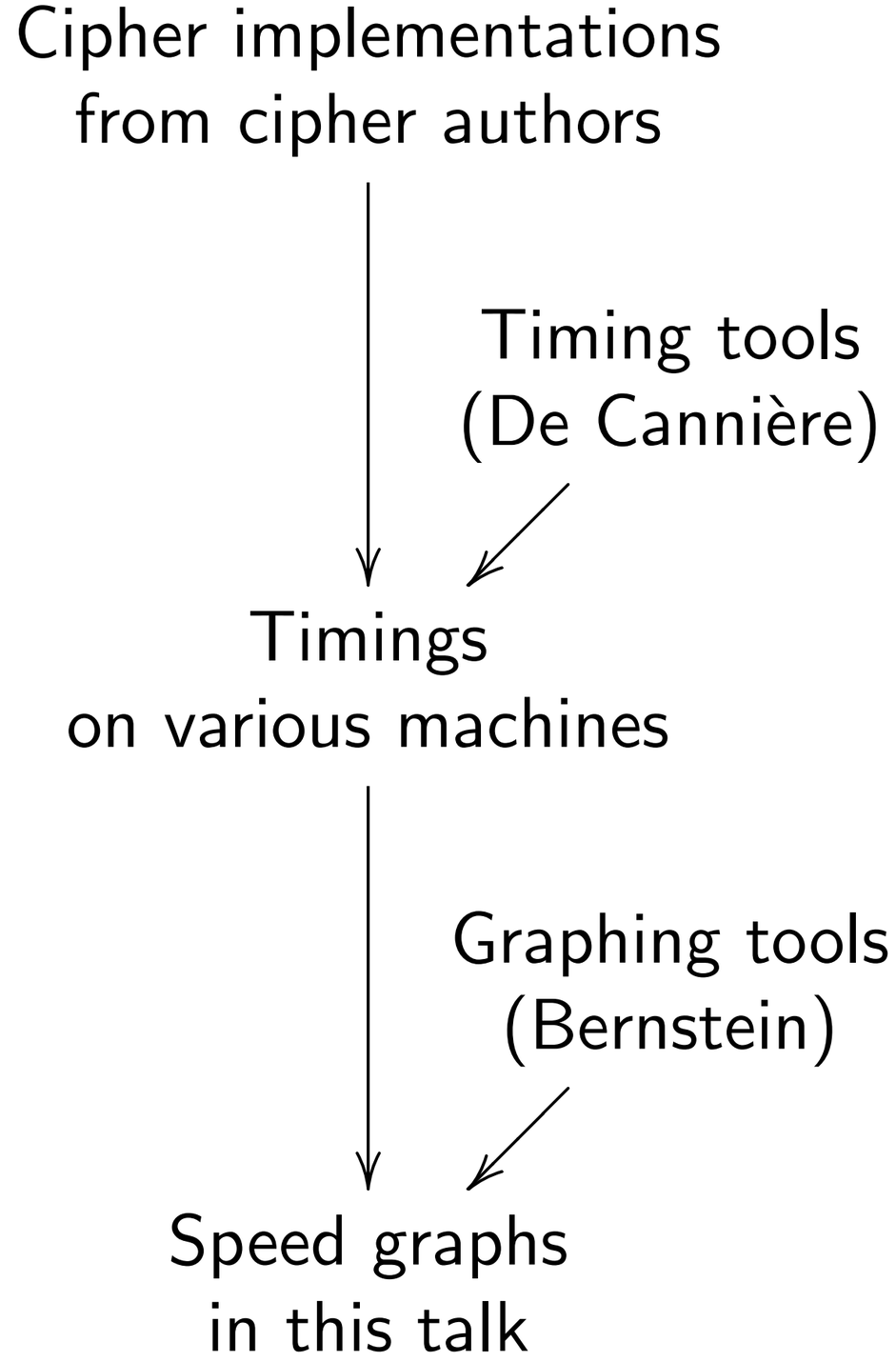
“2^{226}.”

Is there any dispu

about these attac

If not: Reject YA

competition for 2



Security disasters

Attack claimed on YAMB: "2^{58}."

Attack claimed on Py: "2^{72}."
Presumably also Py6.

Attack claimed on SOSEMANUK:
"2^{226}."

Is there any dispute
about these attacks?
If not: Reject YAMB etc. as
competition for 256-bit AES.

tations
thors

Timing tools
De Cannière)

chines

raphing tools
(Bernstein)

hs
k

Security disasters

Attack claimed on YAMB: "2^{58}."

Attack claimed on Py: "2^{72}."
Presumably also Py6.

Attack claimed on SOSEMANUK:
"2^{226}."

Is there any dispute
about these attacks?
If not: Reject YAMB etc. as
competition for 256-bit AES.

Speed disasters

FUBUKI is slower
in all of these ben
Any hope of faste
If not: Reject FU

VEST is extremel
in all of these ben
On the other han
VEST is claimed
faster in hardware

Security disasters

Attack claimed on YAMB: "2^{58}."

Attack claimed on Py: "2^{72}."
Presumably also Py6.

Attack claimed on SOSEMANUK:
"2^{226}."

Is there any dispute
about these attacks?
If not: Reject YAMB etc. as
competition for 256-bit AES.

Speed disasters

FUBUKI is slower than AES
in all of these benchmarks.
Any hope of faster FUBUKI?
If not: Reject FUBUKI.

VEST is extremely slow
in all of these benchmarks.
On the other hand,
VEST is claimed to be
faster in hardware.

n YAMB: "2^{58}."

n Py: "2^{72}."
Py6.

n SOSEMANUK:

ute
cks?
MB etc. as
56-bit AES.

Speed disasters

FUBUKI is slower than AES
in all of these benchmarks.
Any hope of faster FUBUKI?
If not: Reject FUBUKI.

VEST is extremely slow
in all of these benchmarks.
On the other hand,
VEST is claimed to be
faster in hardware.

Remaining 256-bi
CryptMT, DICIN
HC-256, Phelix, S

Could say, e.g.,
"CryptMT is prac
slower than Phelix
and should be elim
but what if Phelix

Attacks on Py, SO
were published in
Need more time f

Speed disasters

FUBUKI is slower than AES
in all of these benchmarks.
Any hope of faster FUBUKI?
If not: Reject FUBUKI.

VEST is extremely slow
in all of these benchmarks.
On the other hand,
VEST is claimed to be
faster in hardware.

Remaining 256-bit ciphers:
CryptMT, DICING, Dragon,
HC-256, Phelix, Salsa20.

Could say, e.g.,
"CryptMT is practically always
slower than Phelix
and should be eliminated";
but what if Phelix is broken?

Attacks on Py, SOSEMANUK
were published in December.
Need more time for cryptanalysis.

r than AES
nchmarks.
er FUBUKI?
BUKI.

y slow
nchmarks.
d,
to be
e.

Remaining 256-bit ciphers:
CryptMT, DICING, Dragon,
HC-256, Phelix, Salsa20.

Could say, e.g.,
"CryptMT is practically always
slower than Phelix
and should be eliminated";
but what if Phelix is broken?

Attacks on Py, SOSEMANUK
were published in December.
Need more time for cryptanalysis.

<u>Speedup: security</u>

Can speed up AE
by reducing round
from 14 to, e.g.,
No known attacks

Can speed up Sal
by reducing round
from 20 to, e.g.,
No known attacks

Do any other sub
have a security m

Remaining 256-bit ciphers:
CryptMT, DICING, Dragon,
HC-256, Phelix, Salsa20.

Could say, e.g.,
"CryptMT is practically always
slower than Phelix
and should be eliminated";
but what if Phelix is broken?

Attacks on Py, SOSEMANUK
were published in December.
Need more time for cryptanalysis.

Speedup: security margin

Can speed up AES
by reducing rounds
from 14 to, e.g., 10.
No known attacks.

Can speed up Salsa20
by reducing rounds
from 20 to, e.g., 12 or 8.
No known attacks.

Do any other submissions
have a security margin?

t ciphers:
G, Dragon,
Salsa20.

ctically always
x
minated";
x is broken?

OSEMANUK
December.
for cryptanalysis.

Speedup: security margin

Can speed up AES
by reducing rounds
from 14 to, e.g., 10.
No known attacks.

Can speed up Salsa20
by reducing rounds
from 20 to, e.g., 12 or 8.
No known attacks.

Do any other submissions
have a security margin?

Slowdown: forger

Packets must be

State of the art:
around 4 cycles p
plus encrypting 1

Fastest encryptio
fastest authentica

Not necessarily!
Phelix includes au

Benchmarks need

Speedup: security margin

Can speed up AES
by reducing rounds
from 14 to, e.g., 10.
No known attacks.

Can speed up Salsa20
by reducing rounds
from 20 to, e.g., 12 or 8.
No known attacks.

Do any other submissions
have a security margin?

Slowdown: forgeries

Packets must be authenticated.

State of the art: Poly1305,
around 4 cycles per byte
plus encrypting 16 bytes.

Fastest encryption implies
fastest authenticated encryption?
Not necessarily!
Phelix includes authentication.

Benchmarks need to cover this.

y margin

S
ds
10.
s.

sa20
ds
12 or 8.
s.

missions
argin?

Slowdown: forgeries

Packets must be authenticated.

State of the art: Poly1305,
around 4 cycles per byte
plus encrypting 16 bytes.

Fastest encryption implies
fastest authenticated encryption?
Not necessarily!
Phelix includes authentication.

Benchmarks need to cover this.

Slowdown: timing

Typical AES softw
leaks key through
Often attacker ca

Constant-time AE
is considerably slo

Slowdown depend
CryptMT, Phelix,
DICING, Dragon,

Benchmarks need

Slowdown: forgeries

Packets must be authenticated.

State of the art: Poly1305,
around 4 cycles per byte
plus encrypting 16 bytes.

Fastest encryption implies
fastest authenticated encryption?
Not necessarily!
Phelix includes authentication.

Benchmarks need to cover this.

Slowdown: timing attacks

Typical AES software
leaks key through timing.
Often attacker can see timing.

Constant-time AES software
is considerably slower.

Slowdown depends on cipher.
CryptMT, Phelix, Salsa20: 0.
DICING, Dragon, HC-256: ?

Benchmarks need to cover this.