Which public-key systems
are smallest? Fastest?

eBATS (ECRYPT Benchmarking
of Asymmetric Systems):
new project to measure
time and space consumed by
public-key signature systems,
public-key encryption systems,
public-key secret-sharing systems.

`http://ebats.cr.yp.to`

Inspired by eSTREAM timings.

eBATS is open to
public submission of BATs
(Benchmarkable Asymmetric
Tools).

e.g. submit encrypting BAT
with three functions:
`keypair()` to generate keys,
`ciphertext()` to encrypt,
`plaintext()` to decrypt.

BATs are measured by BATMAN
(Benchmarking of Asymmetric
Tools on Multiple Architectures,
Non-Interactively).

ECRYPT

y systems
stest?

T Benchmarking
ystems):
neasure
consumed by
ure systems,
ption systems,
-sharing systems.

cr.yp.to

REAM timings.

eBATS is open to
public submission of BATs
(Benchmarkable Asymmetric
Tools).

e.g. submit encrypting BAT
with three functions:
`keypair()` to generate keys,
`ciphertext()` to encrypt,
`plaintext()` to decrypt.

BATs are measured by BATMAN
(Benchmarking of Asymmetric
Tools on Multiple Architectures,
Non-Interactively).

Measured BATs
(Comparison and
Environment).

eBATS is open to public submission of BATs (Benchmarkable Asymmetric Tools).

e.g. submit encrypting BAT with three functions: `keypair()` to generate keys, `ciphertext()` to encrypt, `plaintext()` to decrypt.

BATs are measured by BATMAN (Benchmarking of Asymmetric Tools on Multiple Architectures, Non-Interactively).

Measured BATs enter the CAVE (Comparison and Visualization Environment).

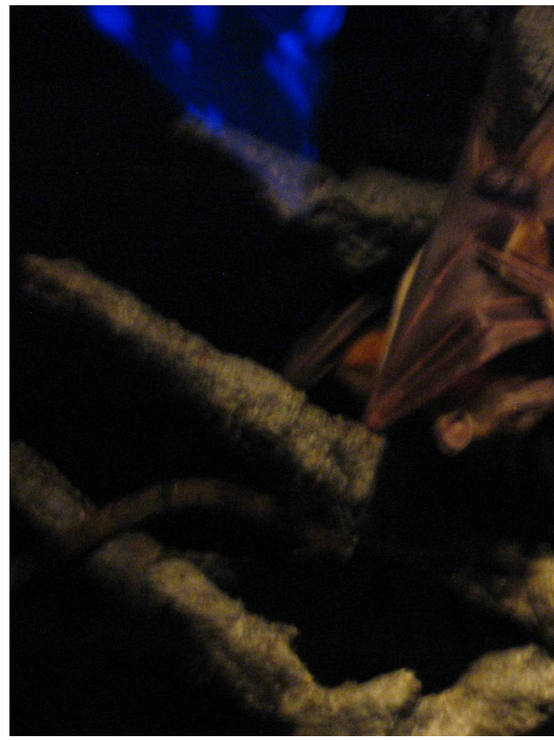
o
n of BATs
Asymmetric

ypting BAT
ons:
enerate keys,
o encrypt,
decrypt.

red by BATMAN
of Asymmetric
e Architectures,
).

Measured BATs enter the CAVE (Comparison and Visualization Environment).

Measured BATs
(Comparison and
Environment).

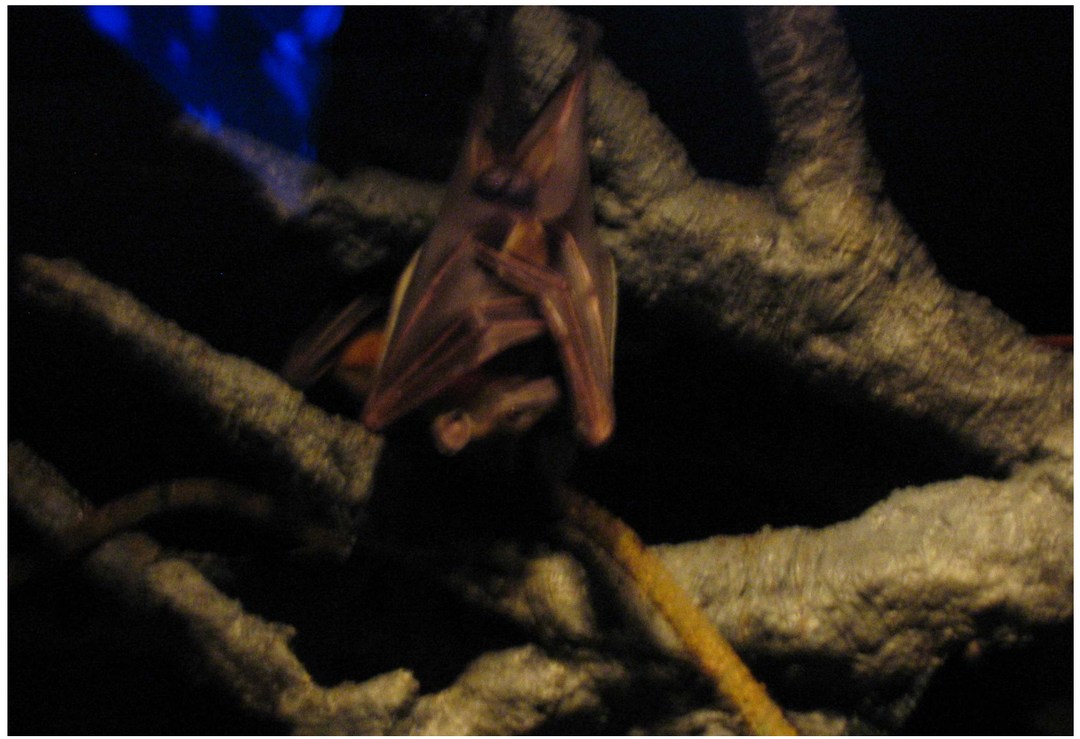


Measured BATs enter the CAVE (Comparison and Visualization Environment).

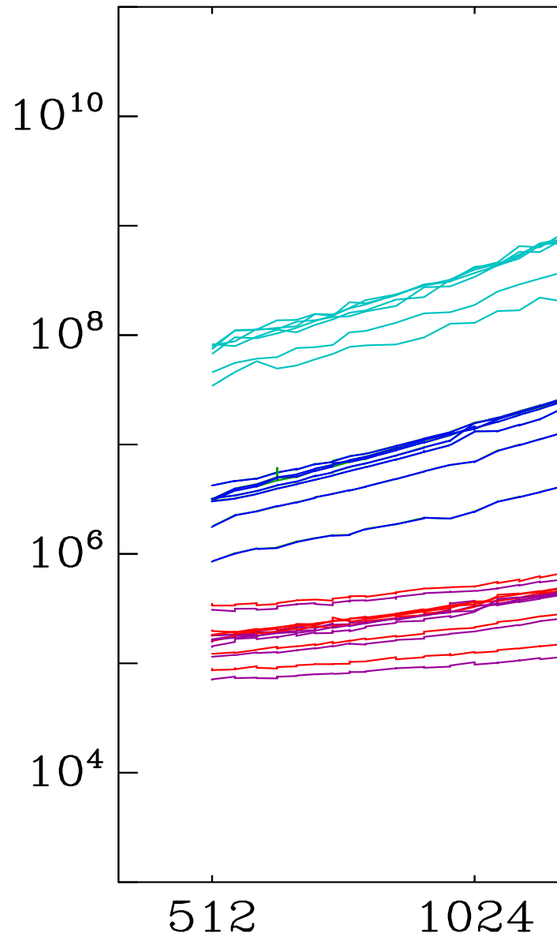
Measured BATs enter the CAVE (Comparison and Visualization Environment).

enter the CAVE
l Visualization

Measured BATs enter the CAVE (Comparison and Visualization Environment).



Measured BATs
(Comparison and
Environment).



Measured BATs enter the CAVE (Comparison and Visualization Environment).

Measured BATs enter the CAVE (Comparison and Visualization Environment).