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.

To join list: `ebats-subscribe@list.cr.yp.to`

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

systems
stest?

T Benchmarking
ystems):
easure
onsumed by
ure systems,
tion systems,
-sharing systems.

`ts-subscribe`
`o`

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).

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).

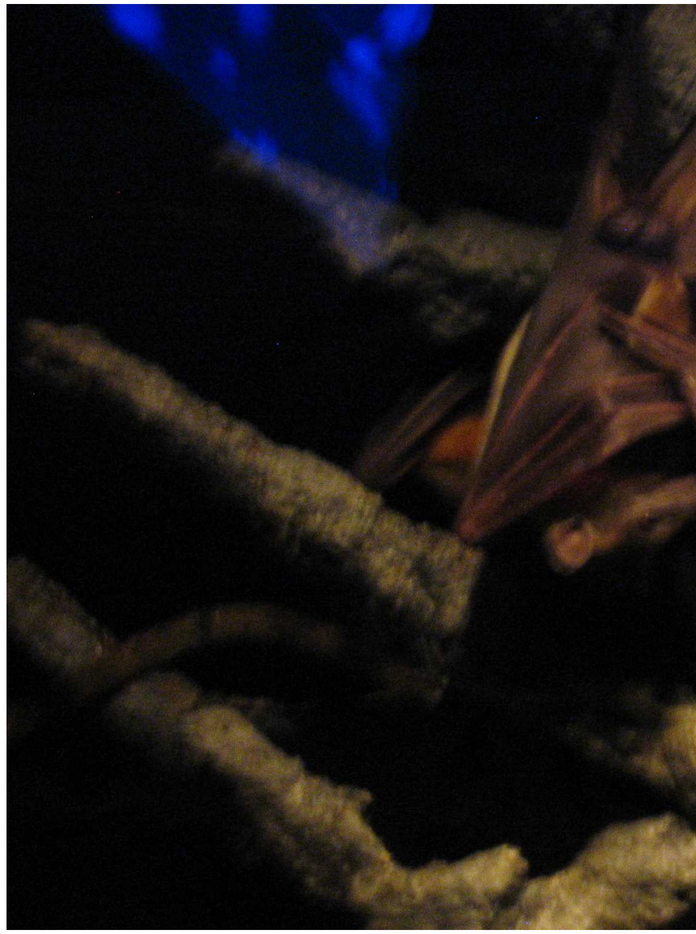
ubmission
markable
ls).

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

red by BATMAN
of Asymmetric
e Architectures,
y).

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

Measured BATs
(Comparison and
Environment).



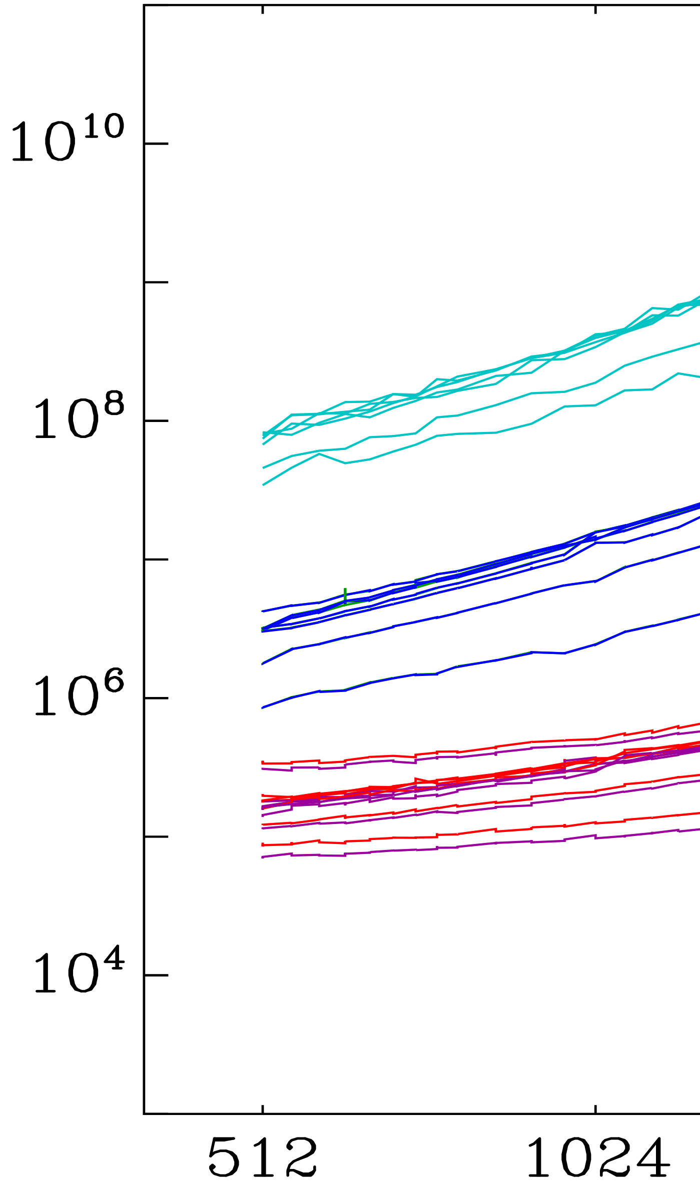
Measured BATs enter the CAVE (Comparison and Visualization Environment).

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

enter the CAVE
Visualization

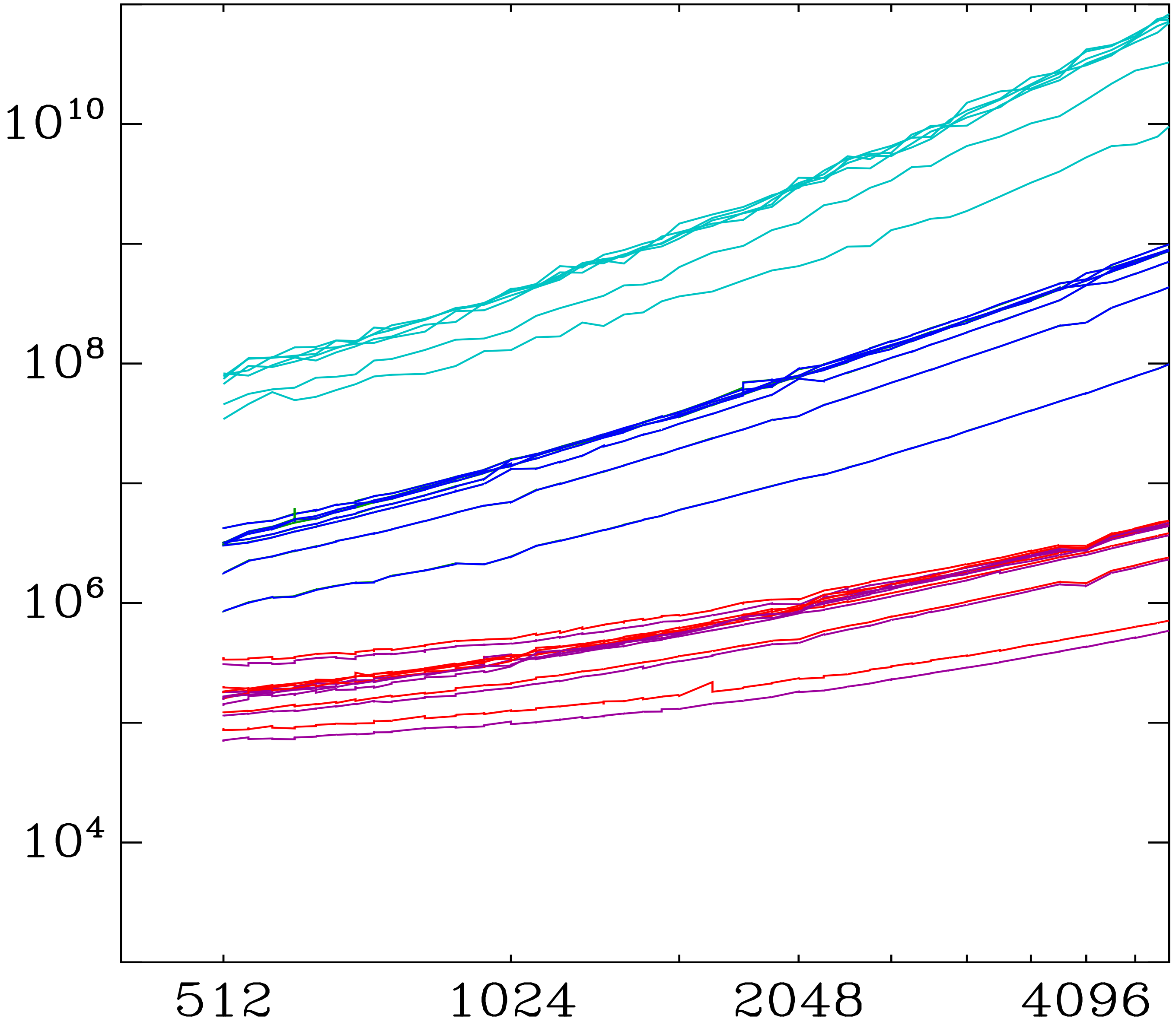
Measured BATs enter the CAVE (Comparison and Visualization Environment).

Measured BATs
(Comparison and
Environment).

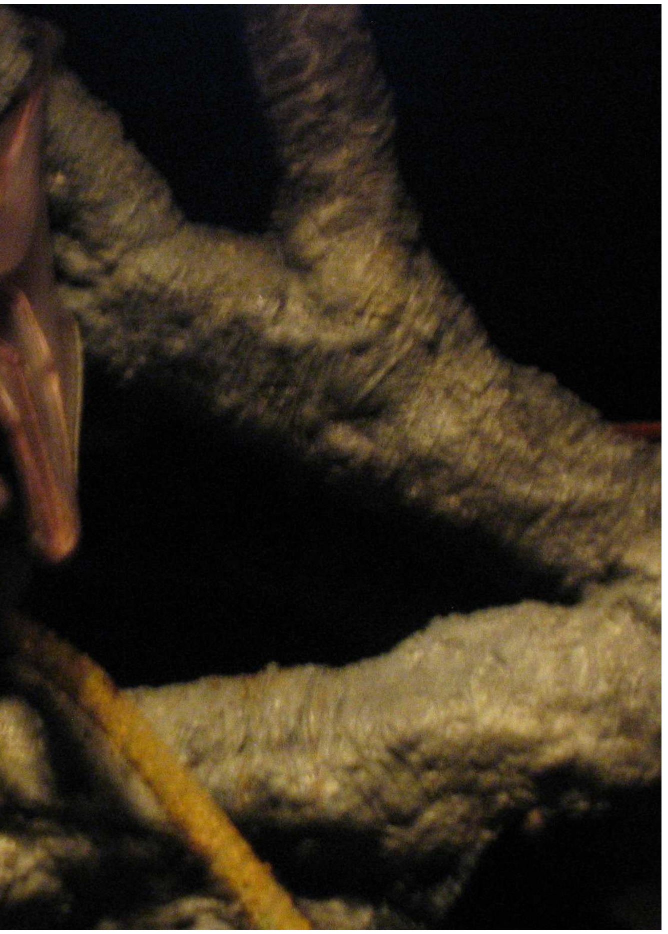


Measured BATs enter the CAVE (Comparison and Visualization Environment).

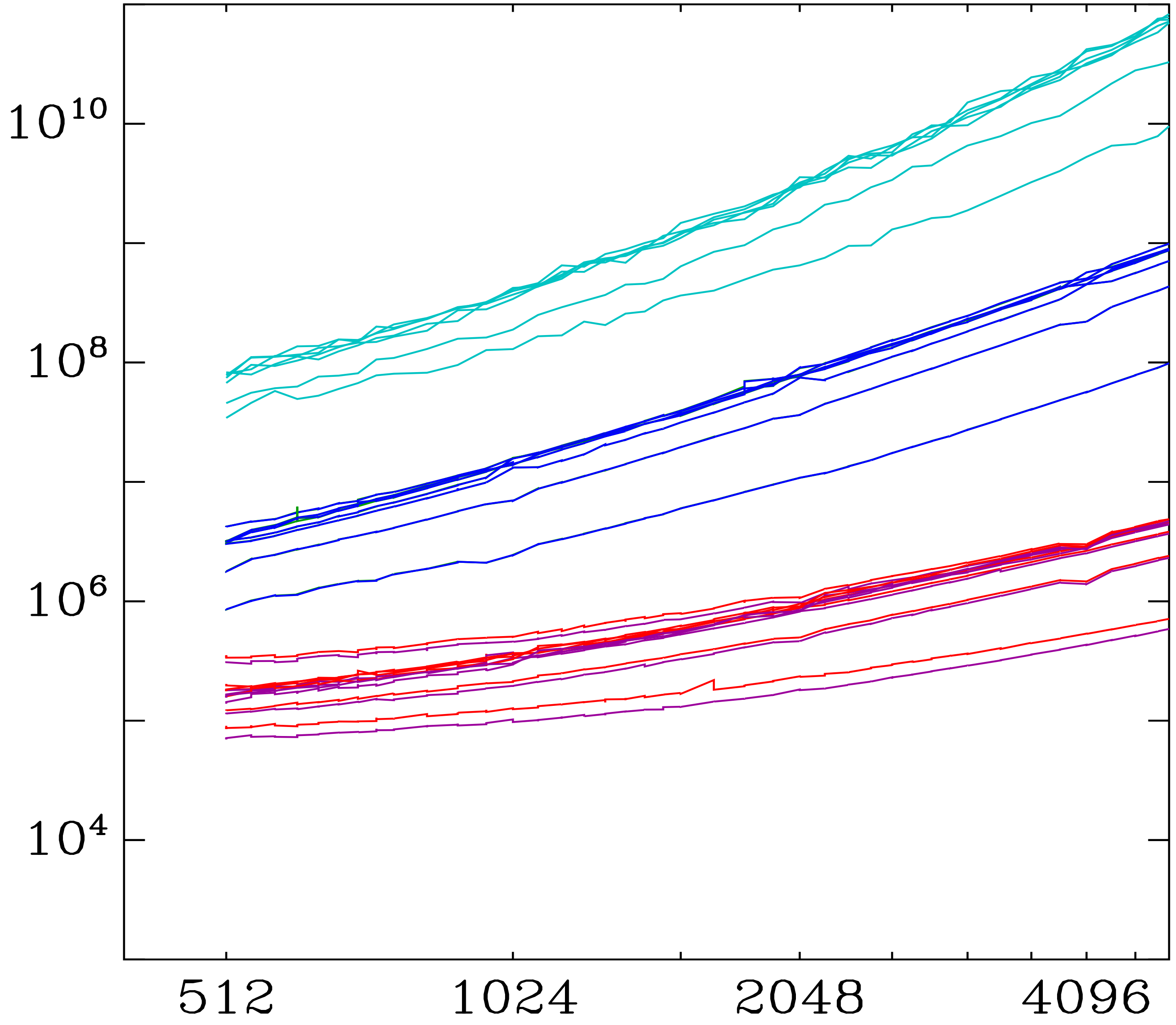
Measured BATs enter the CAVE (Comparison and Visualization Environment).



enter the CAVE
l Visualization



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



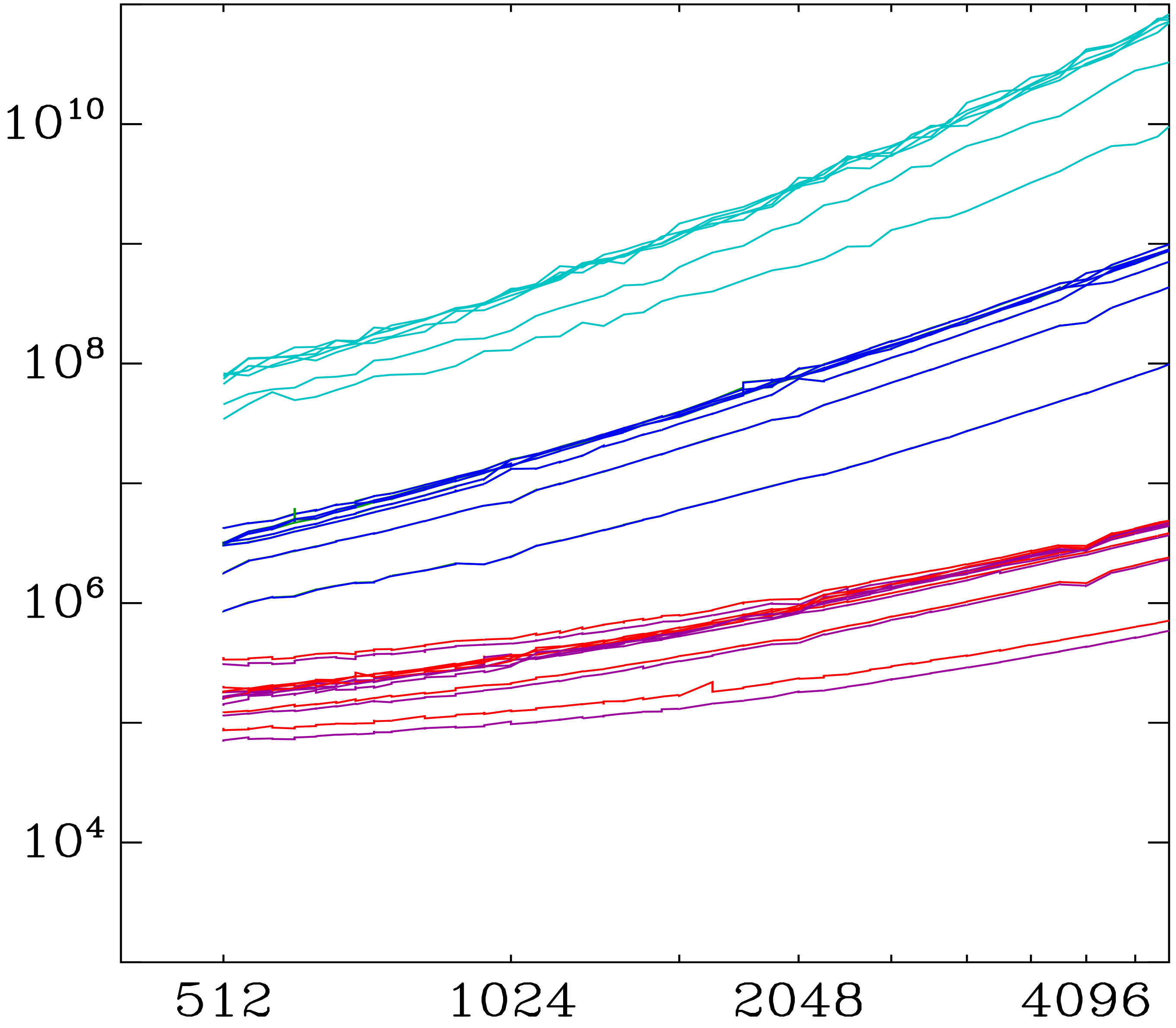
The SHARCS co
Do users *want* th
smallest, fastest

Not exactly! Use
smallest, fastest
at an acceptable

Open to public e
of security levels.

Need papers ana
costs of attacks a
all of these syste

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



The SHARCS connection: Do users *want* the smallest, fastest systems?

Not exactly! Users want the smallest, fastest systems *at an acceptable security level*.

Open to public evaluation of security levels.

Need papers analyzing costs of attacks against all of these systems.