eBATS

ECRYPT Benchmarking of Asymmetric Systems

Daniel J. Bernstein
University of Illinois at Chicago
USA
djb@cr.yp.to

Tanja Lange
Technical University of Denmark
Denmark
tanja@hyperelliptic.org

Users of public-key cryptography have a choice of public-key cryptosystems, including RSA, DSA, ECDSA, and many more. Exactly how fast are these systems? How do the speeds vary among Pentium, PowerPC, etc.? How much network bandwidth do the systems consume?

eBATS (ECRYPT Benchmarking of Asymmetric Systems) aims to answer these questions. The eBATS competition will identify the most efficient public-key systems among the submitted BATs (Benchmarkable Asymmetric Tools). Please submit your BAT according to the following API.

Encrypting BAT

supports the following three functions:

- `keypair` returning a secret key and a public key;
- `ciphertext` reading a message and a public key, returning an encrypted message;
- `plaintext` reading an encrypted message and a secret key, returning the message that was encrypted.

Signing BAT

supports the following three functions:

- `keypair` returning a secret key and a public key;
- `signedmessage` reading a message and a secret key, returning a signed message;
- `messagesigned` verifying a signed message and a public key, returning the message that was signed.

Secret sharing BAT

supports the following three functions:

- `keypair` returning a secret key and a public key;
- `sharedsecret` reading a secret key and another public key, returning a shared secret.

BATMAN

(Benchmarking of Asymmetric Tools on Multiple Architectures, Non-Interactively)

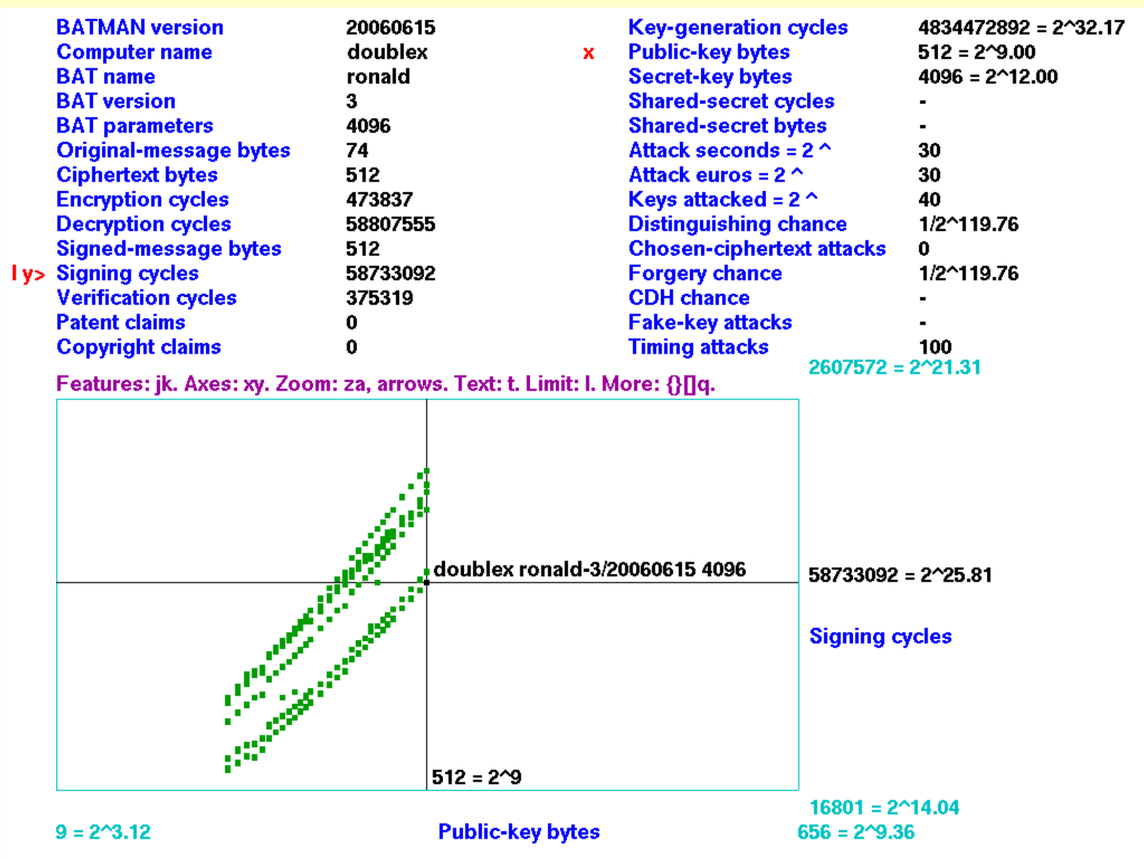
collects measurements of the submitted BATs. It allows a large number of BATs to be systematically measured on a large number of computers. The output of BATMAN is an extensive database of measurements in a form suitable for easy computer processing.

BATMAN is available for download at `http://www.ecrypt.eu.org/ebats/` so that you can benchmark your own BAT and check whether it fits to the API.

Results

BATMAN's results on timings (generate a key, encryption, signing or secret sharing) and sizes (lengths of the keys, length of the ciphertext or signature) are stored in a huge database.

```
20060615 gggg 20060618 claus 1 - - gcc_-mcpu=G5_-O2_-fomit-frame-pointer 4.0.2_20050808_(prerelease)_(Ubuntu_4.0.1-4ubuntu9) sharedsecret - bytes - 128 128 128 128 128 128 128 128 128 128 128 128 128 128 128
20060615 gggg 20060618 claus 1 - - gcc_-mcpu=G5_-O2_-fomit-frame-pointer 4.0.2_20050808_(prerelease)_(Ubuntu_4.0.1-4ubuntu9) sharedsecret - cycles powerpclinux 32862640 32789072 32870016 32797776 32870096 32854352 32794096 32866528 328
20060615 gggg 20060618 claus 1 - - gcc_-mcpu=G5_-O2_-fomit-frame-pointer 4.0.2_20050808_(prerelease)_(Ubuntu_4.0.1-4ubuntu9) sharedsecret - bytes - 128 128 128 128 128 128 128 128 128 128 128 128 128 128 128
20060615 gggg 20060618 claus 1 - - gcc_-mcpu=G5_-O2_-fomit-frame-pointer 4.0.2_20050808_(prerelease)_(Ubuntu_4.0.1-4ubuntu9) sharedsecret - cycles powerpclinux 32877728 32791568 32877728 32874496 32792256 33070800 32908432 32856000 332
20060615 gggg 20060618 claus 1 - - gcc_-mcpu=G5_-O2_-fomit-frame-pointer 4.0.2_20050808_(prerelease)_(Ubuntu_4.0.1-4ubuntu9) sharedsecret - bytes - 128 128 128 128 128 128 128 128 128 128 128 128 128 128 128
20060615 gggg 20060618 claus 1 - - gcc_-mcpu=G5_-O2_-fomit-frame-pointer 4.0.2_20050808_(prerelease)_(Ubuntu_4.0.1-4ubuntu9) cdhchance - chance - 65536 0 0 65536 65536 65536 65536 65536 65536 65536 65536 65536 65536 65536 65536 6
20060615 gggg 20060623 ronald 3 3584 - gcc 4.0.2_20050808_(prerelease)_(Ubuntu_4.0.1-4ubuntu9) forgerychance - chance - 30989 22 20 36365 36109 35853 35597 35341 35085 34829 34573 34317 34061 33805 33549 33293 33037 32781 32525 32269 3
20060615 gggg 20060623 ronald 3 3584 - gcc 4.0.2_20050808_(prerelease)_(Ubuntu_4.0.1-4ubuntu9) forgerychance - chance - 30989 22 24 36365 36109 35853 35597 35341 35085 34829 34573 34317 34061 33805 33549 33293 33037 32781 32525 32269 3
20060615 gggg 20060623 ronald 3 3584 - gcc 4.0.2_20050808_(prerelease)_(Ubuntu_4.0.1-4ubuntu9) forgerychance - chance - 30989 22 28 36365 36109 35853 35597 35341 35085 34829 34573 34317 34061 33805 33549 33293 33037 32781 32525 32269 3
```



CAVE

(Comparison and Visualization Environment)

allows users to dynamically explore various graphs of BATMAN output, sliding between selected slices and projections of the database.

For more details on the API and to download BATMAN and CAVE visit
`http://www.ecrypt.eu.org/ebats/`