SFLASH, a fast asymmetric signature scheme for low-cost smartcards

Implementation

Jacques Patarin, Nicolas Courtois, Louis Goubin

Bull CP8
68 route de Versailles - BP 45
78431 Louveciennes Cedex
France
J.Patarin@frlv.bull.fr, courtois@minrank.org, Louis.Goubin@bull.net

1 Introduction

Implementation is supllied in the form of C++ program that uses Victor Shoup's NTL library.
NTL provides state of the art algorithms for factoring polynomials over finte fields.
The implementation is (apparently) written in ANSI C++.
The source is now tested to compile and work correctly with respect to all tests on the following platforms:
1. Under Windows 9x with Microsoft Visual Studio (we provide the project file NessHfe.dsp).
2. Under Linux/g++ (with Makefile).
Both Linux/Windows cases work OK on a Pentium processor.
3. The source is known not to be portable on a big-endian machine (e.g. sparc) This should be addressed in ulterior versions
Authors wish to thank Louis Granboulan for extensive help.

2 Principle of the implementation

The general philosophy of the program is the following:
The main file is NessHfe.cpp.
There is a single executable that will be called NessHfe.exe or so (system and compiler-dependent).
This file is used in a command-line way.
The output directory in windows should be "C:\Program Files\Multivariate Signature".

Important: The executable NessHfe.exe must be lauched in the directory containing the public or secret key described later.

The program implements potentially many multivariate schemes in such a way that the main program remains the same, and all the algorithm-dependent information for signature generation and verification is stored in a file written in a standard way and that contains not only the public or secret key but also a description of the algorithm.

The public key should be a file with extension .PKey. It is done according to a standard described in the document PKey.ps.
The secret key should be a file with extension .SKey. It is done in a less standart way that is not published, and is always encrypted with RC6.
This philosophy of design allows pro-active approach to the signature: we may add a new algorithm without changing the implementation.
Let || be the string concatenation operation.

2.1 Generation of a pair of public/secret key

To generate a pair of public/secret key we first chose an Id string S with at most 8 charactes or numbers, for example S="Nessie". We write a following command:
NessHfe.exe setup Sflash S
The program will ask for a long string that is hashed with SHA-1 and supplied for NTL's random number genrator (using MD5).
This part takes up to few minutes on a PC and since it is done only once in the lifetime of the signature, it has not been fully optimized yet.
Two files denoted S||".Pkey" and S||".Skey" will be written in the working directory of the program (for example Nessie.PKey and Nessie.SKey). The last is encrypted.

2.2 Generation of a signature

To generate a signature we write a command:
NessHfe.exe S sign FileNameWithOptionalFullPath
This requires the presence of S||".Skey" in the current directory, and the knowledge of the password.
Every file is treated as a binary file and one must be careful about comparing results of signatures of a file.
The signature is displayed and also written to certif.txt. It is deterministic.

2.3 Verification of a signature

To verify a signature we write a command:
NessHfe.exe S check FileNameWithOptionalFullPath
This requires the presence of S||".Pkey" in the current directory.
The program displays if the signature is valid or not, and it returns 1 if invalid and 0 if valid. If something wrong happens, a different return code is returned, -1 is when command line parameters are not correct.

3 Test vectors

Made with our original windows executable included in .\windows\

3.1 Tests on key generation

Parameters used in our test value:

- The password for all keys (it is used later for other tests) must be 0123456789
- The e-mail adress must be entered as default "submissions@cryptonessie.org" (case sensitive)

- The random string must be the default "40db189e97485c3d9a5d5ca11246e49b1c3ad065"
- The key number must be 0 (the default value)

The resulting files *.SKey and *.PKey must be identical to ours.
The test is done on 3 following examples (files generated in those 3 are used for the following verifications).

```
-----------------------------------------------------------------
Command line:
NessHfe.exe setup Sflash Sflash
The resulting files are Sflash.SKey (Md5=d22cb81536ce26381ea59fadbb1aedfd)
and Sflash.Pkey (Md5 will be different at each time because
the public key contains the time at which it was generated).
```

3.2 Tests on signatures

They contain 3 pairs of public/secret keys, 3 files to test signatures on. The password for all keys is 0123456789

```
-----------------------------------------------------------------
Comand line:
NessHfe.exe Sflash sign check.txt

Resulting signature:
06f22ca8288dd2059d5e6601f6c57222c08fc95205a68e39604fc514e30550aec3

Check with command line:
NessHfe.exe Sflash check  check.txt 06f22ca8288dd2059d5e6601f6c
57222c08fc95205a68e39604fc514e30550aec3
-----------------------------------------------------------------
Comand line:
NessHfe.exe Sflash sign test.txt

Resulting signature:
021715221d0504916609a7c04ed7c50c201a9f5568c47202e70c5ffcc25620003b

Check with command line:
NessHfe.exe Sflash check test.txt 021715221d0504916609a7c04ed7
c50c201a9f5568c47202e70c5ffcc25620003b
-----------------------------------------------------------------
Comand line:
NessHfe.exe Sflash sign verify.txt

Resulting signature:
01a2ae8983426315585c4660960c51cad29e678bbbbcd830570717a9362e3ab304

Check with command line:
NessHfe.exe Sflash check verify.txt 01a2ae8983426315585c4660960c
51cad29e678bbbbcd830570717a9362e3ab304
```

4 Practical working with Windows

The working directory in windows should be
"C:\Program Files\Multivariate Signature"
The executable filename must be "C:\Program Files\Multivariate Signature\NessHfe.exe"
Double-click Install.reg to register the program !
The three .bat files supplied should also be in "C:\Program Files\Multivariate Signature". Use them to generate keys.
When we right-click on a file, we have a possibility to sign/check signatures for the SFLASH scheme.