SFLASH, a fast asymmetric signature scheme

Statement Issued by the Authors

Nicolas T. Courtois\textsuperscript{1}, Louis Goubin\textsuperscript{1} and Jacques Patarin\textsuperscript{2}

\textsuperscript{1}Axalto Cryptographic Research & Advanced Security, 
36-38 rue de la Princesse, BP 45, 78430 Louveciennes Cedex, France 
courtois@minrank.org, LGoubin@slb.com

\textsuperscript{2} PRISM, University of Versailles, France Jacques.Patarin@prism.uvsq.fr

1 Support of SFLASH\textsuperscript{v2}

The revised signature scheme SFLASH\textsuperscript{v2} is one of the three asymmetric signature schemes recommended by the Nessie European consortium for low-cost smart cards (cf. NESSIE Portfolio of recommended cryptographic primitives, 
https://www.cosic.esat.kuleuven.ac.be/nessie/deliverables/decision-final.pdf). As the authors of SFLASH, we would like to state that we do no longer recommend the usage of SFLASH\textsuperscript{v2}.

2 New Version SFLASH\textsuperscript{v3}

The parameters of SFLASH have\textsuperscript{1} to be increased: instead of 26 equations with 37 variables over $GF(2^7)$ we recommend to use a version of SFLASH with 56 equations with 67 variables over $GF(2^7)$. We also recommend to modify the hashing procedure as it was suggested by Nessie evaluation reports. A detailed specification of the new version SFLASH\textsuperscript{v3}, is available at http://eprint.iacr.org/.

The new version of SFLASH\textsuperscript{v3} becomes the only version of SFLASH endorsed by the authors. We certify that SFLASH\textsuperscript{v3} is free of any deliberate hidden weakness. The best attack we are aware of on SFLASH\textsuperscript{v3} requires at least about $2^{100}$ CPU operations and we do not believe that there is a much faster method.

It should be noted that the intellectual property status of SFLASH\textsuperscript{v3} is identical to SFLASH\textsuperscript{v2}, cf. https://www.cosic.esat.kuleuven.ac.be/nessie/ipstatements/.

Louveciennes, France, October 2nd 2003,

Nicolas T. Courtois \hspace{1cm} Louis Goubin \hspace{1cm} Jacques Patarin

\textsuperscript{1}This is due to recent improved algorithms for solving random systems of quadratic equations (a.k.a. MQ problem) over $GF(2^k), k > 1$, that are not public at the time of writing [Anonymous communication].