Titolo Volume
ISBN 000-00-000-0000-0
DOI 10.4399/00000000000001
pag. 11–?? (xx 9999)

A new isogeny-based lossy identification protocol for a tightly secure digital signature

Federico Pintore

1. Introduction

Reduction-based security proofs are commonly used in Public-key Cryptography. Given a cryptosystem Π and a mathematical problem $\mathcal{P}$ supposed to be hard, a reduction-based proof shows that an adversary $\mathcal{A}$ able to break Π with success probability ϵ_Π can solve $\mathcal{P}$ with a success probability $\epsilon_\mathcal{P}$. Ideally, $\epsilon_\mathcal{P}$ is approximately ϵ_Π. However, in most security proofs $\epsilon_\mathcal{P}$ is significantly smaller than ϵ_Π.

The recent advancements in quantum computing have led cryptographers to construct schemes whose security is based on mathematical problems believed to be hard even for quantum computers. Isogeny-based Cryptography is a recent line of research which exploits isogenies between elliptic curves to design quantum-resistant cryptographic systems.

While isogeny problems offer compact and efficient solutions to key-exchange protocols [2, 5], they resulted to be rather elusive to use for constructing digital signature schemes. Indeed, while the first practical key-exchange scheme, SIDH [5], appeared in 2011, it was only in mid-2019 that the first practical digital signature, CSI-FiSh [1], was proposed.

CSI-FiSh is obtained by applying the Fiat-Shamir transform [4] to an identification protocol derived from a free and transitive action $\star$ of an abelian finite group $\mathbb{G}$, having order N and generator g, on a set $\mathcal{S}$ of supersingular elliptic curves. Fiat-Shamir signatures are notorious for having a very *loose reduction*[1] in both the random

1. A loose reduction is a reduction-based security proof where $\epsilon_\mathcal{P}$ is far smaller than ϵ_Π, which makes the security proof almost meaningless.

oracle model (ROM)[2] and in the quantum ROM (QROM), and CSI-FiSh makes no exception.

1.1. Our contribution

Since the application of the Fiat-Shamir transform to a *lossy* identification protocol gives rise to a digital signature which enjoys a *tight* security proof[3] (see [6]), we introduce a new lossy identification protocol for the action $\star$. This protocol determines a variant of CSI-FiSh having better security guarantees and almost the same efficiency.

2. A new lossy identification protocol

An identification protocol is a three-move interactive protocol between a prover P and a verifier V. The goal of the interaction is that of making P proving to V that they possess the private key sk corresponding to a given public key pk. The interaction terminates with a proof generated by P, and it must not reveal any information about sk.

In a lossy identification protocol, the set of public keys $\mathcal{PK}$ contains some *lossy keys*, i.e. keys for which the corresponding secret key does not exist. These lossy keys are required to be indistinguishable from proper public keys. Furthermore, any (possibly computationally unbounded) adversary must have a negligible success probability in producing a valid proof for a lossy key.

In the new lossy identification protocol we propose, the set of secret keys $\mathcal{SK}$ coincides with $\mathbb{Z}_N$, while $\mathcal{PK}$ is the set $\mathcal{S}^4$ (where $\mathcal{S}$ is the set on which $\mathbb{G}$ acts). The public key pk corresponding to the secret key $\mathsf{sk} = a \in \mathbb{Z}_N$ is defined as the quadruple (E_1, E_2, F_1, F_2) where E_1, E_2 are random elements in $\mathcal{S}$ and $F_i = g^a \star E_i$ for $i = 1, 2$. It is evident that not all the quadruples in $\mathcal{S}^4$ are proper public keys, i.e. $\mathcal{S}^4$ contains lossy keys.

2. Informally, the ROM is an ideal model where any hash function H is a proper uniformly-random function. Within security proofs given in the ROM, each player has to query an oracle to evaluate the function H.

3. A *tight* security proof is a reduction-based security proof where $\epsilon_\Pi \approx \epsilon_\mathcal{P}$.

The interaction between a prover P, who possesses the secret-public keys pair $(a, (E_1, E_2, F_1, F_2))$, and a verifier V, who is given the public key (E_1, E_2, F_1, F_2), proceeds by repeating t times the following exchange, indexed by $i \in \{1, \ldots, t\}$:

— P uniformly samples an element $r_i \in \mathbb{Z}_N$ and computes the commitment $\mathsf{com}_i = (g^{r_i} \star E_1, g^{r_i} \star E_2)$. P sends com_i to $\mathcal{V}$;
— $\mathcal{V}$ uniformly samples a bit ch_i and sends it to $\mathcal{P}$;
— $\mathcal{P}$ responds with $\mathsf{rsp}_i = r_i$ if $\mathsf{ch}_i = 0$, with $\mathsf{rsp}_i = r_i - a$ if $\mathsf{ch}_i = 1$.

The proof provided by $\mathcal{P}$ is $(\mathsf{rsp}_1, \ldots, \mathsf{rsp}_t)$, which is considered valid by $\mathcal{V}$ if, for every $i \in \{1, \ldots, t\}$, it holds that $(g^{\mathsf{rsp}_i} \star E_1, g^{\mathsf{rsp}_i} \star E_2) = \mathsf{com}_i$ when $\mathsf{ch}_i = 0$, and $(g^{\mathsf{rsp}_i} \star F_1, g^{\mathsf{rsp}_i} \star F_2) = \mathsf{com}_i$ when $\mathsf{ch}_i = 1$.

It is possible to show that the success probability of an adversary $\mathcal{A}$ in producing a valid proof for a lossy key pk is negligible, and, assuming the hardness of a decisional variant of a standard isogeny-based problem, that lossy keys are indistinguishable from proper public keys.

3. Conclusion

Building on the lossy identification protocol described above, El Kaafarani, Katsumata and Pintore proposed a new signature scheme, named Lossy CSI-FiSh [3]. The signature scheme is a variant of CSI-FiSh which is tightly secure in both the ROM and QROM, and it is almost as efficient as CSI-FiSh. In particular, compared to CSI-FiSh, the signature size is the same, the public key is only twice as large, and the runtime of the signature generation and verification is estimated to be (at most) twice as slow.

Titolo Volume
ISBN 000-00-000-0000-0
DOI 10.4399/00000000000002
pag. 15–15 (xx 9999)

Bibliografia

[1] Beullens, W., Kleinjung, T., Vercauteren, F., CSI-FiSh: efficient isogeny based signatures through class group computations, International Conference on the Theory and Application of Cryptology and Information Security, 2019, 227–247, Springer, Cham.

[2] Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J., CSIDH: an efficient post-quantum commutative group action, International Conference on the Theory and Application of Cryptology and Information Security, 2018, 395–427, Springer, Cham.

[3] El Kaafarani, A., Katsumata, S., Pintore, F., Lossy CSI-FiSh: Efficient signature scheme with tight reduction to decisional CSIDH-512, IACR International Conference on Public-Key Cryptography, 2020, 157–186, Springer, Cham.

[4] Fiat, A., Shamir, A., How to prove yourself: Practical solutions to identification and signature problems. Conference on the theory and application of cryptographic techniques, 1986, 186–194, Springer, Berlin, Heidelberg.

[5] Jao, D., De Feo, L., Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, International Workshop on Post-Quantum Cryptography, 2011, 19–34, Springer, Berlin, Heidelberg.

[6] Kiltz, E., Lyubashevsky, V., Schaffner, C., A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model, Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2018, 552–586, Springer, Cham.