A Short-List of Pairing-Friendly Curves Resistant to the Special TNFS at 192-Bit Security Level

Diego F. Aranha[1], Georgios Fotiadis[2], and Aurore Guillevic*[3]

[1]Aarhus University – Danemark
[2]Université du Luxembourg – Luxembourg
[3]Inria Nancy – Université de Lorraine, CNRS, Inria, LORIA, F-54000, Nancy, France – France

Résumé

At WRACH'2019 I presented a simulator developed with Shashank Singh (IISER Bhopal) of the new extended Tower variant (Kim–Barbulescu) of the Number Field Sieve (NFS) algorithm to compute discrete logarithms in extension fields GF(pˆk), and the consequences for pairing-based cryptography: many pairing-friendly curves saw their security decrease, to compensate, their key-sizes shall be enlarged. As an example, the BN-254 curve believed to offer 128 bits of security is re-evaluated at around 103 bits. BLS12-381 is now the leader pairing-friendly curve at 128-bits.
The situation is less definitive at the 192-bit security level and we present a systematic evaluation of security and performences of pairing-friendly elliptic curves of embedding degrees 16 to 28 at the 192-bit security level. We select a short-list thanks to SageMath simulations and estimates, then we benchmark within the RELIC toolkit the most promising curves.

Joint work with Diego F. Aranha, Aarhus University, and Georgios Fotiadis, Université du Luxembourg.

*Intervenant