On the applicability of one method of elliptic curve discrete logarithm problem over prime fields to the Russian standardized curves

E.K. Alekseev, V.D. Nikolaev, S.V. Smyshlyaev

Factor bases algorithms for solving ECDLP

By 2015 several factor bases algorithms for ECDLP were proposed (mainly for $\mathbb{F}_{2^n}$, including potentially subexponential methods).

In 2016 Petit, Kosters and Messeng introduced a new method for solving ECDLP over $\mathbb{F}_p$.

The provided method

No exact complexity estimations made by the authors.

The curves over $\mathbb{F}_p$, where $p - 1 = r \prod_{i=1}^{n'} p_i$, $p_i < B$, B is «small», $r \ll p$, are potentially vulnerable.

Example: NIST P-224: $p = 2^{224} - 2^{96} + 1 \implies p - 1 = 2^{96} \cdot r$.

Applicability to the Russian curves

Examined curves

- Recommendations of the Technical Committee 26;
- RFC 4357;
- RFC 7836.

The criteria for the algorithm parameters, which have to be met in order to overcome standard Pollard's ρ-method, were estimated.

These criteria are not met for any of examined curves.

Results

The standardized Russian elliptic curves are not vulnerable to the attack.

Thank you for your attention.

Questions?