Weakness of $\mathbb{F}_{3^{6 \cdot 509}}$ for Discrete Logarithm Cryptography

Gora Adj, Alfred Menezes*, Thomaz Oliveira and Francisco Rodríguez-Henríquez

CINVESTAV-IPN

*University of Waterloo

Crypto 2013 Rump session - August 20, 2013

Discrete logarithms over small char $\mathbb{F}_{q^n}$: Cryptographic importance

Efficient discrete log algorithms in small char $\mathbb{F}_{q^n}$ fields have a direct negative impact on the security level that small characteristic symmetric pairings can offer:

1. Supersingular elliptic curves over $\mathbb{F}_{2^n}$ with embedding degree $k = 4$
2. Supersingular elliptic curves over $\mathbb{F}_{3^n}$ with embedding degree $k = 6$
3. Supersingular genus-two curves over $\mathbb{F}_{2^n}$ with embedding degree $k = 12$

Define a subexponential-time algorithm as one whose running time is of the form,

$$L_Q[\alpha, c] = e^{c(\log Q)^{\alpha}(\log\log Q)^{1-\alpha}},$$

where $Q = q^n$, q a small prime and $0 < \alpha < 1$, and c is a constant.
$\alpha = 0$: polynomial $\alpha = 1$: fully exponential

Discrete logarithms over small char $\mathbb{F}_{q^n}$: Main developments in the last 30+ years

- Hellman-Reyneri 1982: Index-calculus $L_Q[\frac{1}{2}, 1.414]$
- Coppersmith 1984: $L_Q[\frac{1}{3}, 1.526]$
- Joux-Lercier (2006): $L_Q[\frac{1}{3}, 1.442]$ when q and n are "balanced"
- Hayashi et al. (2012): Used an improved version of the Joux-Lercier method to compute discrete logs over the field $\mathbb{F}_{3^{6\cdot 97}}$
- Joux (2012): $L_Q[\frac{1}{3}, 0.961]$ when q and n are "balanced"
- Joux (2013): $L_Q[\frac{1}{4} + o(1), c]$ when $Q = q^{2m}$ and $q \approx m$
- Göloğlu et al. (2013): somewhat similar to Joux 2013
- Barbulescu-Gaudry-Joux-Thomé (June 19 2013)
  A Quasi Polynomial time Algorithm (QPA), $(\log Q)^{O(\log \log Q)}$,
  faster than $L_Q[\alpha, c]$ for any $\alpha > 0$ and $c > 0$

A mainstream belief in the crypto community

- Several records broken in rapid succession by Joux, Göloğlu et al. and the Caramel team, the last of the series as of today: a discrete log computation over $\mathbb{F}_{2^{6128}} = \mathbb{F}_{(2^8)^{3\cdot257}}$ Joux (May 21, 2013)

A mainstream belief in the crypto community

- Several records broken in rapid succession by Joux, Göloğlu et al. and the Caramel team, the last of the series as of today: a discrete log computation over $\mathbb{F}_{2^{6128}} = \mathbb{F}_{(2^8)^{3\cdot 257}}$ Joux (May 21, 2013)
- As a consequence of these astonishing results, a mainstream belief in the crypto community is that small characteristic symmetric pairings are broken, both in theory and in practice

A mainstream belief in the crypto community

- Several records broken in rapid succession by Joux, Göloğlu et al. and the Caramel team, the last of the series as of today: a discrete log computation over $\mathbb{F}_{2^{6128}} = \mathbb{F}_{(2^8)^{3\cdot 257}}$ Joux (May 21, 2013)
- As a consequence of these astonishing results, a mainstream belief in the crypto community is that small characteristic symmetric pairings are broken, both in theory and in practice
- More than that, some distinguished researchers have expressed in blogs/chats the opinion that all these new developments may sooner or later bring fatal consequences for integer factorization, which eventually would lead to the death of RSA

A mainstream belief in the crypto community

- Several records broken in rapid succession by Joux, Göloğlu et al. and the Caramel team, the last of the series as of today: a discrete log computation over $\mathbb{F}_{2^{6128}} = \mathbb{F}_{(2^8)^{3\cdot 257}}$ Joux (May 21, 2013)
- As a consequence of these astonishing results, a mainstream belief in the crypto community is that small characteristic symmetric pairings are broken, both in theory and in practice
- More than that, some distinguished researchers have expressed in blogs/chats the opinion that all these new developments may sooner or later bring fatal consequences for integer factorization, which eventually would lead to the death of RSA
- Nevertheless, none of the records mentioned above have attacked finite field extensions that have been previously proposed for performing pairing-based cryptography in small char

Our question

Our question: can the new attacks or a combination of them be effectively applied to compute discrete logs in finite field extensions of interest in pairing-based cryptography?

A positive answer: Announcing the weak field $\mathbb{F}_{3^{6\cdot 509}}$

Finding logarithms of linear polynomials	
Relation generation	$2^{22} M_r$
Linear algebra	$2^{48} M_r$
Finding logarithms of irreducible quadratic polynomials	
Relation generation	$2^{50} M_r$
Linear algebra	$2^{67} M_r$
Descent	
Continued-fraction (254 to 30)	$2^{71} M_r$
Classical (30 to 15)	$2^{71} M_r$
Classical (15 to 11)	$2^{73} M_r$
QPA (11 to 7)	$2^{63} M_r$
Gröbner bases (7 to 4)	$2^{65} M_r$
Gröbner bases (4 to 3)	$2^{64} M_r$
Gröbner bases (3 to 2)	$2^{69} M_r$

Table: Estimated costs of the main steps of the new DLP algorithm for computing discrete logarithms in $\mathbb{F}_{(3^6)^{2\cdot 509}}$. M_r denotes the costs of a multiplication modulo the 804-bit prime $r = (3^{509} - 3^{255} + 1)/7$. We also assume that 2^{22} multiplications modulo r can be performed in 1 second

Mixed positive/negative answers for other fields

- When applied to the fields $\mathbb{F}_{2^{12\cdot 367}}$ and $\mathbb{F}_{2^{12\cdot 439}}$, the new algorithm renders a complexity slightly worse than the old Joux-Lercier method. However, the new method is much more amenable for parallelization, and it is expected to outperform Joux-Lercier provided that a massive number of processors (e.g., 2^{30} processors) are at the disposition of the attacker

Mixed positive/negative answers for other fields

- When applied to the fields $\mathbb{F}_{2^{12\cdot367}}$ and $\mathbb{F}_{2^{12\cdot439}}$, the new algorithm renders a complexity slightly worse than the old Joux-Lercier method. However, the new method is much more amenable for parallelization, and it is expected to outperform Joux-Lercier provided that a massive number of processors (e.g., 2^{30} processors) are at the disposition of the attacker
- Our preliminary analysis suggests that the new algorithm is ineffective for computing discrete logs in $\mathbb{F}_{2^{4\cdot1223}}$, a field that not long ago was assumed to offer a security level of 128 bits

Mixed positive/negative answers for other fields

- When applied to the fields $\mathbb{F}_{2^{12\cdot 367}}$ and $\mathbb{F}_{2^{12\cdot 439}}$, the new algorithm renders a complexity slightly worse than the old Joux-Lercier method. However, the new method is much more amenable for parallelization, and it is expected to outperform Joux-Lercier provided that a massive number of processors (e.g., 2^{30} processors) are at the disposition of the attacker
- Our preliminary analysis suggests that the new algorithm is ineffective for computing discrete logs in $\mathbb{F}_{2^{4\cdot 1223}}$, a field that not long ago was assumed to offer a security level of 128 bits
  (Maybe it still does!)

Mixed positive/negative answers for other fields

- When applied to the fields $\mathbb{F}_{2^{12\cdot 367}}$ and $\mathbb{F}_{2^{12\cdot 439}}$, the new algorithm renders a complexity slightly worse than the old Joux-Lercier method. However, the new method is much more amenable for parallelization, and it is expected to outperform Joux-Lercier provided that a massive number of processors (e.g., 2^{30} processors) are at the disposition of the attacker
- Our preliminary analysis suggests that the new algorithm is ineffective for computing discrete logs in $\mathbb{F}_{2^{4\cdot 1223}}$, a field that not long ago was assumed to offer a security level of 128 bits
(Maybe it still does!)
- All the technical details are discussed in the eprint report 2013/446