An interesting result without any cryptological implications

Claus Diem

University of Leipzig

The result

There exists a sequence of finite fields of increasing size over which the elliptic curve discrete logarithm problem can be solved in subexponential time.

The result

Theorem. Let $\epsilon > 0$. Then one can solve the discrete logarithm problem in elliptic curves over finite fields of the form $\mathbb{F}_{q^n}$ with $(2+\epsilon) \cdot n^2 \leq \log_2(q)$ in an expected time which is polynomial in q.

The result

Corollary. Let again $\epsilon > 0$, and let $a > 2 + \epsilon$. Then one can solve the discrete logarithm problem in elliptic curves over finite fields of the form $\mathbb{F}_{q^n}$ with

$$(2 + \epsilon) \cdot n^2 \leq \log_2(q) \leq a \cdot n^2$$

in an expected time of

$$e^{\mathcal{O}(1) \cdot (\log(q^n))^{2/3}} \ .$$

The result

Corollary. Let again $\epsilon > 0$, and let $a > 2 + \epsilon$. Then one can solve the discrete logarithm problem in elliptic curves over finite fields of the form $\mathbb{F}_{q^n}$ with

$$(2 + \epsilon) \cdot n^2 \leq \log_2(q) \leq a \cdot n^2$$

in an expected time of

$$e^{\mathcal{O}(1) \cdot (\log(q^n))^{2/3}} .$$

Indeed, the expected running time is polynomial in

$$q = 2^{\log_2(q)} = 2^{(\log_2(q))^{(1+1/2) \cdot 2/3}} \leq 2^{(\sqrt{a} \cdot n \log_2(q))^{2/3}} .$$

Good and bad news

The bad news.

Good and bad news

The bad news.

The proof is long (over 40 pages), and uses quite a few concepts from arithmetic algebraic geometry like:

Good and bad news

The bad news.

The proof is long (over 40 pages), and uses quite a few concepts from arithmetic algebraic geometry like:

Schemes, sheaves, toric varieties, intersection theory, and general resultants.

Good and bad news

The bad news.

The proof is long (over 40 pages), and uses quite a few concepts from arithmetic algebraic geometry like:

Schemes, sheaves, toric varieties, intersection theory, and general resultants.

The good news.

Good and bad news

The bad news.

The proof is long (over 40 pages), and uses quite a few concepts from arithmetic algebraic geometry like:

Schemes, sheaves, toric varieties, intersection theory, and general resultants.

The good news.

Let us define “cryptology” as the science of designing and analyzing cryptographic systems.

Good and bad news

The bad news.

The proof is long (over 40 pages), and uses quite a few concepts from arithmetic algebraic geometry like:

Schemes, sheaves, toric varieties, intersection theory, and general resultants.

The good news.

Let us define “cryptology” as the science of designing and analyzing cryptographic systems. Then:

This is a mathematical result, not a cryptological one.

Good and bad news

The bad news.

The proof is long (over 40 pages), and uses quite a few concepts from arithmetic algebraic geometry like:

Schemes, sheaves, toric varieties, intersection theory, and general resultants.

The good news.

Let us define “cryptology” as the science of designing and analyzing cryptographic systems. Then:

This is a mathematical result, not a cryptological one.

There are no cryptological implications of the result.

Good and bad news

The bad news.

The proof is long (over 40 pages), and uses quite a few concepts from arithmetic algebraic geometry like:

Schemes, sheaves, toric varieties, intersection theory, and general resultants.

The good news.

Let us define “cryptology” as the science of designing and analyzing cryptographic systems. Then:

This is a mathematical result, not a cryptological one.

There are no cryptological implications of the result.

A question

Why was the result presented at the Rump Session of Eurocrypt 2008?