Degustazione of the ECDLP

Steven Galbraith

University of Auckland, New Zealand

Menu

- Aperitivo: Pohlig-Hellman
- Antipasto: Baby-step-giant-step
- Primo: Pollard rho and kangaroo
- Secondo: Summation polynomials and the ECDLP

Please interrupt me and ask questions. This will aid digestion.

Pohlig-Hellman

- Let G be a group and H a normal subgroup. Let $\phi : G \to G/H$ be the quotient map $\phi(g) = gH$.
  If $h = g^a$ in G then $\phi(h) = \phi(g)^a$ in G/H.
- Everyone knows that one can use this idea to reduce the DLP in a cyclic group G to the DLP in subgroups.
- Combining Chinese remainder theorem and Hensel lifting allows to solve DLP by reducing to DLPs in groups of prime order.
- Hence, we usually work in subgroup of prime order.

Computational Diffie-Hellman problem and Pohlig-Hellman

- The Computational Diffie-Hellman problem (CDH) is: Given g, g^a, g^b to compute g^{ab}.
- Suppose G is a group of order pq where p and q are distinct primes.
- Then can solve CDH by reducing to CDH in cyclic subgroups of order p and q respectively:

  $$\text{CDH}(g^p, g^{ap}, g^{bp}) = g^{abp} \quad \text{and} \quad \text{CDH}(g^q, g^{aq}, g^{bq}) = g^{abq}$$

  from which we can deduce g^{ab} using integers s and t with $sp + tq = 1$.
- **Question:** What about a cyclic group G of order p^2?

Textbook Baby-step-giant-step (BSGS)

- Let P have order r and $Q = aP$.
  Let $N = \lceil \sqrt{r} \rceil$. Then $a = a_0 + Na_1$ with $0 \le a_0, a_1 < N$.
- BSGS is to compute sorted list of all "baby steps" (aP, a) for $0 \le a < N$.
  Let $P' = NP$. Compute "giant steps" $Q - bP'$ for $b = 0, 1, 2, \ldots$ until get a match.
- The worst-case running time is $2\sqrt{N}$ group operations, and average case is $1.5\sqrt{N}$ group operations.
- What more needs to be said?

Baby-step-giant-step

NOTE: Some of the numbers in this table will likely change!

Algorithm	Average-case	Worst-case
Textbook BSGS	1.5	2.0
Textbook BSGS for av. case	1.414	2.121
Pollard BSGS	1.333	2.0
Bernstein-Lange grumpy giants	1.2*	1.73?
Rho	1.253	∞
BSGS with negation	1.0	1.5
Pollard BSGS with negation	0.943	1.414
Grumpy giants with negation	0.84?	?
New	0.666 – 0.748	1.06
Grumpy giants + new	0.6 – 0.678?	?

(Joint with Ping Wang and Fangguo Zhang)

New method

- Computing $P_1 + P_2$ on an elliptic curve using affine coordinates requires $I + 2M + S$.
- Computing $P_1 + P_2$ and $P_1 - P_2$ together requires $I + 4M + 2S$.
- So organise BSGS to store x-coordinates only and to compute the giant steps in blocks.
- For example: Let $P' = NP$ and $P'' = 3P'$. Let $S = Q$. At each iteration compute $S \pm P'$ and then $S = S + P''$. In other words, at iteration i have $S = Q + (3i)P'$ and we consider $\{S{-}P', S, S{+}P'\} = \{Q{+}(3i{-}1)P', Q{+}(3i)P', Q{+}(3i{+}1)P'\}$.
- **Question:** Can we do this trick with Pollard rho?

Some (not very) recent work

- S. D. Galbraith and R. S. Ruprai, An improvement to the Gaudry-Schost algorithm for multidimensional discrete logarithm problems, IMA International Conference on Cryptography and Coding 2009.
- S. D. Galbraith and R. S. Ruprai, Using equivalence classes to speed up the discrete logarithm problem in a short interval, PKC 2010.
- S. D. Galbraith and M. Holmes, A non-uniform birthday problem with applications to discrete logarithms, Discrete Applied Mathematics 2012.
- S. D. Galbraith, J. M. Pollard and R. S. Ruprai, Computing discrete logarithms in an interval, Math. Comp. 2013.

Random walk algorithms

- DLP: Given g, h in group of order r, find a such that $h = g^a$.
- Idea: If can find integers a_1, a_2, b_1, b_2 such that

  $$g^{a_1} h^{b_1} \;=\; g^{a_2} h^{b_2}.$$

  then solve the DLP as $a = (a_2 - a_1)(b_1 - b_2)^{-1} \pmod{r}$.
- Generate pseudorandom sequences

  $$x_i \;=\; g^{a_i} h^{b_i}$$

  such that (a_i, b_i) are known.
- A **collision** is when $x_i = x_j$.
- **Pollard's big idea**: use pseudorandom walks where the next step only depends on the current position.
  Hence, if $x_i = x_j$ then $x_{i+1} = x_{j+1}$.
- Detect collisions without storing all points.

Two basic types of walk

- DLP: Given g, h, find a such that $h = g^a$.
- **First type**: Elements of walks are

$$x_i \;=\; g^{a_i} h^{b_i}$$

  where a_i and b_i are “pseudorandom”.
  Any collision $x_i = x_j$ is potentially useful. Such algorithms are analysed using the birthday paradox.
- **Second type**: Walks are either **tame** $x_i \;=\; g^{a_i}$ or **wild** $y_j \;=\; hg^{b_j}$.
- A collision $x_i = y_j$ allows to solve the DLP as $h = g^{a_i - b_j}$.
  Collisions $x_i = x_j$ or $y_i = y_j$ are useless.
  Such algorithms are analysed using several notions in probability theory.

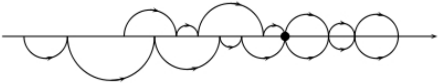
Birthday paradox

- Suppose we sample uniformly at random from a set of size N. The expected number of trials until an element is sampled twice is $\sqrt{\pi N/2}$.
- When $N = 365$ this expected number is ≈ 23.94.
- Now sample uniformly at random from a set of size N and record each element in one of two lists.
  The expected number of trials until an element appears in both lists is $\sqrt{\pi N}$.
- The expected number of people in a room before there is a boy and a girl with the same birthday is ≈ 33.86.
- **Puzzle:** In my hotel there is a meeting of the “boys born in January” club, and a meeting of the “random girls” club. What ratio of each should I put in a room to have a boy and girl with the same birthday? (As $31 \to \infty$.)

The DLP in an Interval

- Given g, h, N find a, if it exists, such that $h = g^a$ and $0 \leq a < N$.
- Applications: breaking pseudorandom generator by Gennaro, decryption in the Boneh-Goh-Nissim scheme, analysis of the static/strong Diffie-Hellman problem, etc.
- Pollard kangaroo method using distinguished points (van Oorschot and Wiener 1996/1999) solves problem in average case expected $(2 + o(1))\sqrt{N}$ group operations.
- **Important:** kangaroo method is not analysed using the birthday paradox.
  Instead, steps in the walk are "short", meaning $x_i = g^{a_i}$ and $x_{i+1} = g^{a_{i+1}}$ is such that $a_{i+1} \approx a_i + m$.

Pollard kangaroo algorithm



- The tame kangaroo starts in the middle of the interval.
- Steps in the walk are, on average, distance m.
- The rear kangaroo "catches up" with the starting point of the front kangaroo in average time $N/(4m)$.
- After about m steps we expect rear kangaroo to land on a footstep of the front kangaroo.
- Average running time $2(N/(4m) + m + o(\sqrt{N}))$.
- Taking $m = \sqrt{N}/2$ gives (av. case expected) running time $(2 + o(1))\sqrt{N}$ group operations.

Improved DLP in an Interval (Math. Comp. 2013)

Two ways to improve:

- Three (actually, four) kangaroos method in $\approx 1.71\sqrt{N}$ group operations.
  Idea is to start wild kangaroos at both h and h^{-1}.
  Walks are now of three types: $x_i = g^{a_i}, \; y_j = hg^{b_j}$ or $z_k = h^{-1}g^{c_k}$.
  A collision between walks of any two types solves the DLP.
  (Assume group order odd.)
- Gaudry-Schost algorithm (cockroaches) in $\approx 1.66\sqrt{N}$ group operations.

Gaudry-Schost Algorithm

- A way to tackle constrained problems using a variant of the birthday paradox.
- One has a “tame set” T and a “wild set” W and seeks collisions in $T \cap W$.
- The random walks are “cockroaches”: staying in an appropriate-sized neighbourhood of the starting point.
- Basic idea for DLP in an interval:

  $$T = \{g^x : 0 \le x < N\}, \quad \text{and} \quad W = \{hg^x : -N/2 < x < N/2\}.$$

  Then $N/2 \le \#(T \cap W) \le N$.
- Model cockroaches as pseudorandom sampling from $T \cap W$. Apply variant of birthday paradox. Average case expected run-time $(2.08 + o(1))\sqrt{N}$ group ops.
- There are some inconvenient aspects.

Equivalence Classes

- Many groups have efficiently computable automorphisms ψ. For example, the map $\psi : g \mapsto g^{-1}$ is easy for elliptic curves and the torus T_2.
- Gallant-Lambert-Vanstone/Wiener-Zuccherato solve the ECDLP by defining a random walk on G/ψ (sets of orbits in the group G under ψ).
- For Pollard rho, using equivalence classes with respect to inversion "should" speed-up the algorithm by a factor of $\sqrt{2}$.

DLP in an Interval Using Equivalence Classes

- It seems impossible to combine Pollard's kangaroo algorithm with equivalence classes.
- But Gaudry-Schost comes to the rescue.
- Analysis uses a generalisation of the Birthday Paradox that was worked out with Mark Holmes.
  (This answers the "January boys" problem.)
- **Theorem:** (G.-Ruprai, PKC 2010) There is an algorithm to solve the DLP in an interval of size N in groups with fast inversion that requires (ignoring troubles with cycles) average expected $(1.36 + o(1))\sqrt{N}$ group operations.
- **Question:** Improve this result, or find an easier-to-implement algorithm than Gaudry-Schost.

Index calculus concept for ECDLP

- Let $P, Q \in E(\mathbb{F}_{q^n})$ be an ECDLP instance.
- Define a suitable factor base $\mathcal{F} \subseteq E(\mathbb{F}_{q^n})$.
- Generate random points $R = aP + bQ$ and try to write

  $$R = P_1 + P_2 + \cdots + P_m$$

  where $P_1, \ldots, P_m \in \mathcal{F}$.
- Each successful **point decomposition** is called a **relation**.
- When enough relations have been computed one can solve the ECDLP using linear algebra.

Point decomposition

- We wish to solve

$$R = P_1 + P_2 + \cdots + P_m \qquad (*)$$

where $P_1, \ldots, P_m \in \mathcal{F}$.

- The right hand side is a rational function in the variables $x_i, y_i \in \mathbb{F}_{q^n}$ such that $P_i = (x_i, y_i) \in E(\mathbb{F}_{q^n})$.
- Hence, solving the equation (*) reduces to solving a system of polynomial equations in $2m$ variables in $\mathbb{F}_{q^n}$.
- It is natural to choose $\mathcal{F}$ to reduce the number of variables.
- Gaudry and Diem used Weil restriction to provide a natural definition for $\mathcal{F}$ that reduces the number of variables while increasing the number of equations.

Semaev's summation polynomials

- Semaev defines, for fixed elliptic curve E, polynomials $\mathrm{Sem}_{m+1}(x_1, \ldots, x_{m+1})$ such that points $R, P_1, \ldots, P_m \in E(\mathbb{F}_{q^n})$ satisfy

  $$R = P_1 + P_2 + \cdots + P_m \qquad (*)$$

  if $\mathrm{Sem}_{m+1}(x(P_1), x(P_2), \ldots, x(P_m), x(R)) = 0$.
- Converse true up to choice of signs.
- Semaev explains how to compute these polynomials and proves they are symmetric and have degree 2^{m-1} in each variable.

Factor base (following Diem)

- Let $V \subseteq \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-vector space of dimension ℓ.
- Define $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in V\}$.
  Then $\#\mathcal{F} \approx q^\ell$.
- We expect approximately $\#\mathcal{F}^m/m! \approx q^{\ell m}/m!$ points of the form $P_1 + \cdots + P_m$ for $P_i \in \mathcal{F}$.
- Hence, a relation (*) exists with probability approximately $q^{\ell m}/(m!q^n)$.
- Solving a relation using Semaev's polynomials and Weil restriction with respect to $\mathbb{F}_{q^n}/\mathbb{F}_q$ requires solving a system with ℓm variables and n equations.

Point decomposition revisited

- The rational function
$$R = P_1 + P_2 + \cdots + P_m \qquad (*)$$
where $P_i = (x_i, y_i) \in E(\mathbb{F}_{q^n})$ has $2m$ variables and the degree is determined by the elliptic curve group law and the degree of the defining equations $y_i^2 = f(x_i)$ of the elliptic curve.
- Semaev's approach is to minimize number of variables at the expense of exponential degree.
- Using projective equations for addition may lead to a larger number of equations, each of lower degree.
- Using elliptic curve equations in higher dimensional spaces also leads to lower degree (but more variables).
- **Question:** What is the optimal tradeoff of number of variables versus degree for point decomposition algorithms?

Other applications of point decomposition

- There exist “delayed target one-more discrete log”, “oracle-assisted static Diffie-Hellman” and “static one-more Diffie-Hellman” problems.
- Given a static (also called “one-sided”) Diffie-Hellman oracle $O(Y) = aY$.
- At some later point would like to compute $Q = aP$ given a random point P.
- Granger (ASIACRYPT 2010) noted that summation polynomials can be used to attack these problems.
- Good news is that only need a small number of point decompositions.
- Also $O(r^{1/3})$ algorithm due to Brown-Gallant/Cheon.

Using symmetries

- Gaudry noted that, since $\mathrm{Sem}_{m+1}(x_1, \ldots, x_m, x(R))$ is invariant under action by symmetric group S_m, one can write it in terms of elementary symmetric polynomials σ_j.
- This leads to a system of equations of lower degree.
- Faugère, Gaudry, Huot and Renault (J. Crypto., 2014) solved system using Gröbner basis with respect to grevlex order (F4 or F5 algorithm) and then FGLM (Faugère, Gianni, Lazard and Mora) change of ordering algorithm.
- They also use invariants under a larger group, coming from action of symmetric group and points of small order.
- This gives improvement to both point decomposition and linear algebra. (But don't forget extra step.)
- Also see the F-H-Joux-R-Vitse paper (EUROCRYPT 2014) and later talks at this meeting.

Larger values for n

- All records done for $E(\mathbb{F}_{q^n})$ where q is medium/large and n is fairly small.
- Then $\mathcal{F}$ is defined using the $\mathbb{F}_q$-vector space $V = \mathbb{F}_q \subseteq \mathbb{F}_{q^n}$, and Weil restriction is defined with respect to $\mathbb{F}_{q^n}/\mathbb{F}_q$.
  Important fact: $x_1, x_2 \in \mathbb{F}_q$ implies $x_1 x_2 \in \mathbb{F}_q$.
  So if $x_1, \dots, x_m \in V$ then $\sigma_j(x_1, \dots, x_m) \in V$.
- No big experiments for the case $E(\mathbb{F}_{2^n})$ where n is prime.
- Huang, Petit, Shinohara and Takagi (IWSEC 2013) study large extension degrees.
- Define factor base using $\mathbb{F}_2$-vector space $V \subset \mathbb{F}_{2^n}$.
  Important fact: $x_1, x_2 \in V \subset \mathbb{F}_{2^n}$ does not imply $x_1 x_2 \in V$.

Huang, Petit, Shinohara and Takagi

- Fix polynomial basis $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ for $\mathbb{F}_{2^n}/\mathbb{F}_2$.
- Choose V to have basis $\{1, \theta, \ldots, \theta^{\ell-1}\}$.
- Then if x_1, x_2 lie in V then $x_1 x_2$ lies in space $V^{(2)}$ with basis $\{1, \theta, \ldots, \theta^{2(\ell-1)}\}$.
- Hence have $\sigma_1 \in V$, $\sigma_2 \in V^{(2)}$, $\sigma_3 \in V^{(3)}$ and so on.
- From some point onwards we have $V^{(j)} = \mathbb{F}_{2^n}$.
- Biggest example in their paper: $n = 53$, $m = 3$, $\ell = 6$, computation takes around 30 seconds.

New work, joint with Shishay Gebregiyorgis

- New choice of invariant variables for binary Edwards curves.
- Factor base that “breaks symmetry” and hence significantly increases the probability that relations exist.
- Experiment with SAT solvers rather than Gröbner basis methods for solving polynomial systems over $\mathbb{F}_2$.

Breaking symmetry

- As noted the symmetric group S_m acts on $R = P_1 + \cdots + P_m$, and hence acts on $\mathrm{Sem}_{m+1}(x(R), x_1, \ldots, x_m)$.
- Good news: We can write this polynomial in terms of elementary symmetric variables and this lowers the degree.
- Bad news: Probability of a relation goes down by $1/m!$.
- Counterintuitive: we can evaluate the symmetric variables at combinations of non-symmetric variables.
- So get benefit of lower degree polynomial equations without the additional $m!$ factor in the running time.

Breaking symmetry

- Precisely: Let $V \subseteq \mathbb{F}_{2^n}$ be a vector space of dimension ℓ.
- Instead of one set $\mathcal{F} = \{P \in E(\mathbb{F}_{2^n}) : x(P) \in V\}$ we define m sets $\mathcal{F}_i = \{P \in E(\mathbb{F}_{2^n}) : x(P) \in V + v_i\}$ where $v_i \in \mathbb{F}_{2^n}$ are elements of a certain form so that the sets $V + v_i$ are all distinct.
- Suppose V has basis $\{1, \theta, \dots, \theta^{\ell-1}\}$.
- Let $v_1 = 0$, $v_1 = \theta^{\ell}$, $v_2 = \theta^{\ell+1}$, $v_3 = \theta^{\ell} + \theta^{\ell+1}$ etc.
- Then $V + v_i$ are distinct and yet only need a couple more variables to represent the combination.
- Hence, we have $\sigma_1 \in V'$ spanned by $\{1, \theta, \dots, \theta^{\ell+1}\}$, $\sigma_2 \in V''$ spanned by $\{1, \theta, \dots, \theta^{2(\ell+1)}\}$ etc.
- Care needed to pull solutions in the σ_j back to solutions in x_j.
- Diem has also used different factor bases $\mathcal{F}_i$.

Conclusion

- SAT solvers are an interesting alternative to Gröbner basis methods and can be faster in some situations.
- But our computations are for small examples (e.g., $n = 53$, $m = 4$ and $\ell = 9$).
- ECDLP in $E(\mathbb{F}_{2^n})$ for prime $n > 160$ seems to be completely immune to point decomposition attacks.
- A practical cube-root-time algorithm for ECDLP (the case $m = 3$) seems hopeless in $E(\mathbb{F}_{2^n})$ when n is prime.
- Even meaningful attacks on one-more/oracle-assisted/static problems seem hopeless since would need to make exponentially many oracle queries.
- **Question:** Is there any way to speed up using Galois action e.g., $E/\mathbb{F}_2$ but ECDLP in $E(\mathbb{F}_{2^n})$?

Dolce

Thanks for your attention.

Answers

- How to solve CDP in group of order p^2 using CDH oracle for groups of prime order?
  Use den Boer/Maurer/Maurer-Wolf reduction to solve DLP.
- Boys in January?
  Minimum of $f(x) = cx(1-x)$ always at $x = \frac{1}{2}$.