Reductions of Problems related to Discrete Logarithms

Frederik Vercauteren
ESAT/COSIC - K.U. Leuven
The Problems

Elliptic Curves

Reductions

Pairings and inversion
Outline

The Problems

Elliptic Curves

Reductions

Pairings and inversion
DLP, CDH & DDH

- Let \((G, \cdot)\) be a finite cyclic group \(G = \langle g \rangle\) of order \(|G|\).

- **Discrete Logarithm Problem (DLP):**
  Given \(h \in G\) find \(x\) with \(h = g^x\) (DLP\((g, h) \rightarrow x\))

- **Computational Diffie-Hellman Problem (CDH):**
  Given \(a = g^x\) and \(b = g^y\) find \(c = g^{xy}\) (CDH\((g, a, b) \rightarrow c\)).

- **Decisional Diffie-Hellman Problem (DDH):**
  Given \(a = g^x, b = g^y\) and \(c = g^z\), determine if
  \[g^{xy} = g^z\] or equivalently \(xy \equiv z \mod |G|\).
  (DDH\((g, a, b, c) \rightarrow true/false\))
DLP & CRT

- Mostly called Pohlig-Hellman algorithm . . .
- Let \(|G| = \prod_{i=0}^{r} p_i^{e_i}\), then can compute DLP using CRT by projection onto subgroups of order \(p_i\)
- If \(h = g^x\), then can compute \(x_{i,0} \equiv x \mod p_i\) by solving

\[
h^{\lvert G \rvert / p_i} = \left( g^{\lvert G \rvert / p_i} \right)^{x_{i,0}}
\]

- Write \(x \equiv \sum_{j=0}^{e_i} x_{i,j} p_i^j \mod p_i^{e_i}\), then can compute \(x_{i,k}\) via

\[
\left( h \cdot g^{-\left(x_{i,0} + \cdots + x_{i,k-1} p_i^{k-1}\right)} \right)^{\lvert G \rvert / p_i^{k+1}} = \left( g^{\lvert G \rvert / p_i} \right)^{x_{i,k}}
\]
DLP & CRT

- DLP in subgroups of order $p_i$ via exhaustive search
- Complexity then is in group operations

$$O(\sum e_i(\log |G| + p_i))$$

- If $G$ is $B$-smooth, i.e. all $p_i \leq B$ then

$$O(\log |G|^2 + \frac{B}{\log B} \log |G|)$$

- If $|G|$ is smooth, then DLP is easy
Reductions

Let $A$ and $B$ be two computational problems. Then $A$ is said to **polytime reduce** to $B$, written $A \leq_P B$ if

- There is an algorithm which solves $A$ using an algorithm which solves $B$.
- This algorithm runs in polynomial time if the algorithm for $B$ does.

Assume we have an oracle (or efficient algorithm) to solve problem $B$.

We then use this oracle to give an efficient algorithm for problem $A$. 
Trivial Reduction I: CDH $\leq_P$ DLP

- Given $g^x$ and $g^y$ we wish to find $g^{xy}$.
- First compute $y = \text{DLP}(g, g^y)$ using the oracle.
- Then compute $(g^x)^y = g^{xy}$.
- So CDH is no harder than DLP, i.e. CDH $\leq_P$ DLP.
Trivial Reduction II: \( \text{DDH} \leq_P \text{CDH} \)

- Given elements \( g^x, g^y \) and \( g^z \), determine if \( g^z = g^{xy} \).
- Using the oracle to solve \( \text{CDH} \), compute
  \[
g^{xy} = \text{CDH}(g, g^x, g^y).
  \]
- Then check whether \( g^{xy} = g^z \).
- So \( \text{DDH} \) is no harder than \( \text{CDH} \), i.e. \( \text{DDH} \leq_P \text{CDH} \).
Trivial Reduction III: I-DHP $\leq_P$ CDH

I-DHP: given $g, g^x$ compute $g^{x^{-1}}$, where $x^{-1}$ is computed modulo $|G|$.

- I-DHP $\leq_P$ CDH with $\log_2 n$ DH-calls:
  - Recall: $x^{-1} \equiv x^{\varphi(|G|) - 1} \mod |G|$
  - Use DH-oracle and square and multiply
  - $\text{CDH}(g, g^x, g^x) = g^{x^2}$ and $\text{CDH}(g, g^{x^s}, g^{x^t}) = g^{x^{s+t}}$

Alternatively:

- I-DHP $\leq_P$ CDH with one DH call:
  - Let $h = g^x$, then $g = h^{x^{-1}}$, so

$$\text{DHP}(h, g, g) = h^{x^{-1} \cdot x^{-1}} = g^{x^{-1}}$$
Reduced: DLP $\leq_P$ CDH

- Assume first that $|G| = q$ a prime.
- Implicit representations (i.e. computing in exponent):

<table>
<thead>
<tr>
<th>Explicit</th>
<th>Implicit</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x$</td>
<td>$g^x$</td>
</tr>
<tr>
<td>$y$</td>
<td>$g^y$</td>
</tr>
<tr>
<td>$x + y \mod q$</td>
<td>$g^x \cdot g^y$</td>
</tr>
<tr>
<td>$x \cdot y \mod q$</td>
<td>CDH($g, g^x, g^y$)</td>
</tr>
</tbody>
</table>

- CDH-oracle enables us to compute implicitly over $\mathbb{F}_q$, $+, \cdot$ or an algebraic group $H$ defined over $\mathbb{F}_q$. 
Crazy idea I: DLP ⩽_P CDH by den Boer

- Assume that \( q - 1 \) is smooth, so DLP in \( \mathbb{F}_q^* \) is easy
- Since \( x \) is determined modulo \( q \), we can write

\[
x \equiv \alpha^s \mod q
\]

for \( \alpha \) a generator modulo \( q \)
- Goal: compute \( s \) instead of \( x \)
- Using Pohlig-Hellman + exhaustive search in the exponent
- Limitation: \( q - 1 \) smooth
Crazy idea II: DLP $\leq_P$ CDH by Maurer-Wolf

- den Boer: only one choice $\mathbb{F}_q^*$ for each $q$
- Maurer-Wolf: DH-oracle combined with other auxiliary groups $H$ over $\mathbb{F}_q$
- Works as long as $x$ or $x + e$ for some known $e$ can be used as “coordinate” of element in $H$ (strongly algebraic group)
- Embed $x$ in element $\beta$ of $H$
- Compute log $s$ of $\beta$ wrt known generator $\alpha \in H$
- Recover $\beta$ and thus $x$ by computing $\alpha^s$
Outline

The Problems

Elliptic Curves

Reductions

Pairings and inversion
Elliptic Curves

- Let $\mathbb{F}_q, +, \cdot$ be a finite field with $q > 3$ a large prime.
- Elliptic curve $E$ over field $\mathbb{F}_q$ is defined by
  \[ y^2 = x^3 + ax + b \quad a, b \in \mathbb{F}_q \]
- The set of $\mathbb{F}_q$-rational points $E(\mathbb{F}_q)$ is defined as
  \[ E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q \mid y^2 = x^3 + ax + b\} \cup \{O\} \]
- $O$ is called point at infinity

There exists an addition law on $E$ and the set $E(\mathbb{F}_q)$ is a group
Addition Law on Elliptic Curves

Adding two points

Doubling a point

\[ y^2 = x^3 - 7x + 6 \]
Addition Law on Elliptic Curves

By definition: three points on a line sum to zero!

Let \( P_1 \oplus P_2 = P_3 \), with \( P_i = (x_i, y_i) \in E \)

- If \( x_1 = x_2 \) and \( y_1 + y_2 = 0 \), then \( P_1 \oplus P_2 = O \),
- Else

\[
\begin{align*}
\lambda & = (y_2 - y_1)/(x_2 - x_1) \\
\nu & = (y_1 x_2 - y_2 x_1)/(x_2 - x_1)
\end{align*}
\]

\[
\begin{align*}
\lambda & = (3x_1^2 + a)/2y_1 \\
\nu & = (-x_1^3 + ax_1 + 2b)/2y_1
\end{align*}
\]

The point \( P_3 = P_1 \oplus P_2 \) is given by

\[
\begin{align*}
x_3 & = \lambda^2 - x_1 - x_2 \\
y_3 & = -\lambda x_3 - \nu
\end{align*}
\]
Elliptic Curves over Finite Fields

The elliptic curve $y^2 = x^3 + x + 3 \mod 23$
Number of Points on Elliptic Curve

- With probability 1/2 we have $x^3 + ax + b$ is square in $\mathbb{F}_q$, and then 2 solutions.
- Expect to find roughly $p$ solutions . . .
- Theorem (Hasse):

$$\#E(\mathbb{F}_q) = q + 1 - t \quad \text{with} \quad |t| \leq 2\sqrt{p}.$$

- Rück: for every $n \in [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$ exists cyclic elliptic curve over $\mathbb{F}_q$ of order $n$. 
Outline

The Problems

Elliptic Curves

Reductions

Pairings and inversion

Frederik Vercauteren  ESAT/COSIC - K.U. Leuven

Reductions of Problems related to Discrete Logarithms
Crazy idea II: DLP $\leq_P$ CDH by Maurer-Wolf

- Auxiliary group = elliptic curve
- Find $E/\mathbb{F}_q$ with $|E(\mathbb{F}_q)|$ smooth and $E(\mathbb{F}_q)$ cyclic
- Let $E(\mathbb{F}_q) = \langle P \rangle$ with $P = (u, v)$
- By calling DH-oracle, find $e$ such that

$$R = (x + e)^3 + a(x + e) + b$$

is square in $\mathbb{F}_q^*$

- Can be tested by computing $R^{(q-1)/2}$ in exponent
- Construct point $Q = (x + e, y)$ in implicit representation
- Compute dlog $s$ of $Q$ wrt $P$ in implicit representation
- Recover $Q$ by computing $[s]P$ and thus $x + e = x(Q)$
Reductions: DLP $\leq_P$ CDH by Maurer-Wolf

- Let $G$ be a finite cyclic group with $|G| = q$
- Given an elliptic curve $E(\mathbb{F}_q)$ with $B$-smooth $|E(\mathbb{F}_q)|$, i.e., all prime factors $p_i | |E(\mathbb{F}_q)|$ are $p_i < B$.
- Given a DH oracle for $G$, then one can compute DLP in $G$ using
  - $O\left(\frac{\log q}{\log B}\right)$ calls to the DH oracle for $G$
  - $O\left(\frac{B}{\log B}(\log q)^2\right)$ field operations in $\mathbb{F}_q$
Reductions: DLP $\leq_P$ CDH by Maurer-Wolf

- To obtain polynomial equivalence, need curve with very smooth order
- Let $\nu(q)$ be minimum of largest prime factor of all integers $n$ in the interval $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$
- Rück: exists elliptic curve $E/\mathbb{F}_q$ with $|E(\mathbb{F}_q)| \nu(q)$-smooth
- Not much is known about smoothness in short intervals
- However: for every $u$, number of $n^{1/u}$ smooth integers $< n$
  \[
  \frac{n}{u^{(1+o(u))u}}
  \]
Reductions: DLP $\leq_P$ CDH by Maurer-Wolf

- Smoothness assumption: $\nu(q)$ is $\log(q)^{O(1)}$
- Conclusion: for all groups $G$ of prime order $q$, there exists an elliptic curve $E/\mathbb{F}_q$ such that DLP $\leq_P$ CDH
- Practice: not really need polynomial time equivalence, weaker result is already sufficient
- Idea: DLP well studied problem, so complexity well understood
- Example: DLP in $E/\mathbb{F}_p$ prime order $q$ requires $O(\sqrt{q})$
Hardness of EC-CDH

- Maurer-Wolf implies $C_{DLP} \leq N_{DH} \cdot C_{CDH} + N_{Muls}$, thus
  $$C_{CDH} \geq \frac{C_{DLP} - N_{Muls}}{N_{DH}}$$

- Given auxiliary curve $E' / \mathbb{F}_q$ with $|E'(\mathbb{F}_q)| = p_1 p_2 p_3$ and $p_i \approx q^{1/3}$, then best algorithm to solve CDH takes
  $$O\left(\frac{\sqrt{q}}{(\log q)^2}\right)$$
Outline

The Problems

Elliptic Curves

Reductions

Pairings and inversion
Computational Diffie-Hellman Problem (CDH): Given $a = g^x$ and $b = g^y$ find $c = g^{xy}$ (CDH($g, a, b$) $\rightarrow$ $c$).

Decisional Diffie-Hellman Problem (DDH): Given $a = g^x$, $b = g^y$ and $c = g^z$, determine if $g^{xy} = g^z$ or equivalently $xy \equiv z \mod |G|$

(DDH($g, a, b, c$) $\rightarrow$ true/false)

Already shown that DDH $\leq_P$ CDH

Can we prove that CDH $\leq_P$ DDH?
Reductions: \( \text{CDH} \leq_P \text{DDH} \)?

- No, since exist groups where DDH is easy, but not CDH
- Take \( E/\mathbb{F}_q \) supersingular elliptic curve and \( r \mid |E(\mathbb{F}_q)| \), then exists bilinear map (aka pairing)

\[
e : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_q)[r] \rightarrow \mu_r : (P, Q) \mapsto e(P, Q)
\]

- Can prove that \( \mu_r \subset \mathbb{F}_{q^6} \) and map can be computed in polynomial time
- To solve DDH in \( E(\mathbb{F}_q)[r] \) given \((P, xP, yP, zP)\) simply

\[
e(P, zP) = e(xP, yP)
\]
Suppose need to solve CDH in $E(\mathbb{F}_q)[r]$, i.e. given $xP$, $yP$ compute $xyP$

Using pairing, compute $e(P, P)^{xy} = \text{solution to CDH but in wrong group!}$

If efficiently computable isomorphism $\phi : \mu_r \to E(\mathbb{F}_q)[r]$ exists, with $\phi(e(P, P)) = P$, then $\phi(e(xP, yP)) = xyP$

Inverse of isomorphisms $e(\cdot, P)$ or $e(P, \cdot)$

How hard is pairing inversion?
Pairing Inversion

- Satoh: hardness result for polynomial expressions
- Let $E$ be an ordinary elliptic curve over $\mathbb{F}_p$, with $r|E(\mathbb{F}_p)$
- Given any isomorphism $\phi : \mu_r \to E(\mathbb{F}_p)[r]$, the polynomial $P \in \overline{\mathbb{F}}_p[z]$ with

$$P(\gamma) = x(\phi(\gamma)) \quad \text{for } \gamma \in \mu_r \setminus \{1\}$$

satisfies:
- $\deg P = (r - 1)/5$ (always)
- for 58% of pairs $(E, r)$, none of the coefficients of $P$ vanishes
Pairing Inversion

- Pairings can have extremely simple form.
- Let $E : y^2 = x^3 + 4$ over $\mathbb{F}_p$ with $p = 41761713112311845269$, then $t = -1$, $r = 715827883$, $k = 31$ and $D = -3$.
- Let $y - \lambda(Q)x - \nu(Q)$ with $\lambda = 3x_Q^2/(2y_Q)$ and $\nu = (-x_Q^3 + 8)/(2y_Q)$ be the tangent at $Q$.
- The function

$$
(Q, P) \mapsto (y_P - \lambda(Q)x_P - \nu(Q))^{(p^k-1)/r}
$$

defines a non-degenerate pairing on $G_2 \times G_1$.
- Pairing inversion = inverting exponentiation $(p^k - 1)/r$
The Problems
Elliptic Curves
Reductions
Pairings and inversion

Hidden Root Problem

- Let \( \mathbb{F}_q \) be a finite field and \( x \in \mathbb{F}_q \) secret
- Fix \( n \) a positive integer with \( n \mid (q - 1) \)
- Oracle: input \( (a, b) \in \mathbb{F}_q^2 \) returns \( \xi_{a,b} = (ax + b)^n \)
- Goal: recover \( x \) by querying oracle
- Let \( s = (q - 1)/n \), then for each query obtain \( \log_2 s \) bits information
- After roughly \( \log_s q \) queries, unique solution \( x \)
- Example: Legendre symbol \( n = (q - 1)/2 \) and \( s = 2 \)
Hidden Root Problem over Extension Fields

- Let \( q = p^k \) for prime some prime \( p \) and \( k > 1 \)
- Fix representation \( \mathbb{F}_{p^k} = \mathbb{F}_p[\theta]/(f(\theta)) \) where \( f \in \mathbb{F}_p[x] \) is an irreducible polynomial of degree \( k \)
- Consider the map

\[
\psi : \mathbb{F}_{p^k} \rightarrow (\mathbb{F}_p)^k : a = \sum_{i=0}^{k-1} a_i \theta^i \mapsto [a_0, \ldots, a_{k-1}]
\]

- Since \( p \)-th powering linear operation, can easily compute matrix \( F \) such that \( \psi(a^p) = F \psi(a)^t \)
Hidden Root Problem over Extension Fields

- Write exponent $n$ as $n = \sum_{i=0}^{k-1} c_i p^i - \sum_{i=0}^{k-1} d_i p^i$ where $c_i, d_i \in \mathbb{N}_{\geq 0}$.
- Each equation $\xi_{a,b} = (ax + b)^n$ then leads to
  \[
  \prod_{i=0}^{k-1} (a^{p^i} x^{p^i} + b^{p^i})^{c_i} = \xi_{a,b} \prod_{i=0}^{k-1} (a^{p^i} x^{p^i} + b^{p^i})^{d_i}.
  \]
- System of $k$ non-linear equations in $k$ unknowns of degree
  \[
  D = \max\{\sum_{i=0}^{k-1} c_i, \sum_{i=0}^{k-1} d_i\}.
  \]
Hidden Root Problem over Extension Fields

- Can be solved in time $\left( D + k \right)^{\omega} \binom{D + k}{D}$ with $\omega \leq 3$ time for matrix multiplication exponent.
- For tiny $D$ this is doable in practice.
- Very few $n$ have tiny $D$.
- Crucial observation: no need to work with $n$ itself, can also use a multiple of $n$ (but not of $p^k - 1$).
Hidden Root Problem over Extension Fields

- How to automagically find best multiple of $n$?
- Consider lattice $L \subset \mathbb{Z}^k$ spanned by the rows

$$L := \begin{pmatrix} n & 0 & 0 & \cdots & 0 \\ -p & 1 & 0 & \cdots & 0 \\ -p^2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -p^{k-1} & 0 & \cdots & 0 & 1 \end{pmatrix}.$$  

- $V \in L$ corresponds to multiple $\langle V, [1, p, \cdots, p^{k-1}] \rangle$.
- Shortest vector in $L$ gives best possible multiple.
Hidden Root Problem over Extension Fields

- Algorithm works well for all divisors of \((p^k-1)/\Phi_k(p)\)
- \(\Phi_k\) is \(k\)-th cyclotomic polynomial
- Unfortunately, does not include exponent appearing in extremely simple pairing
- Possible to define pairing of the form

\[ e : G_2 \times G_1 \rightarrow \mu_r : (Q, P) \mapsto f_{S,Q}(P)^{(p^k-1)/\Phi_k(p)} \]

but then function \(f_{S,Q}\) too complicated (roughly degree \(r\))
Conclusions

- Maurer-Wolf: $\text{CDH} \equiv_P \text{DLP}$ when given good auxiliary elliptic curves
- Practice: obtain bounds on hardness of CDH using easy to find curves
- $\text{DDH} <_P \text{CDH}$ in groups with bilinear pairing
- Pairing inversion would give easy CDH and thus DLP
- So far: only negative results . . .