A MOR cryptosystem built on extra-special p-groups

Ayan Mahalanobis

Indian Institute of Science Education and Research, Pune

April 16, 2011

The discrete logarithm problem

- Let $G = \langle g \rangle$ be a cyclic group.
- For $x \in [1, |G|]$, g and g^x is known.
- The problem is to find x.

An Example

Take for an example, the group as $\mathbb{F}_{2341}^{\times} = \langle 7 \rangle$. We are given 7 and 1564 and the question is: find the x such that $7^x = 1564$. The answer is 1321.

The problem can be described in any group. However, it is not secure in any group.

- The problem is known to be hard (hardest?) in the group of rational points of an elliptic curve.
- It is trivial in $(\mathbb{Z}_n +)$.

Question: What makes the discrete logarithm problem hard?

The Diffie-Hellman key exchange protocol

Alice and Bob wants to communicate over an insecure channel. They pick a cyclic group $G = \langle g \rangle$.

- Alice picks a $a \in [1, |G|]$, computes g^a and send that to Bob.
- Bob on the other hand computes g^b and sends it to Alice.
- Both of them can compute g^{ab} which they can use as a private key.

The security of the Diffie-Hellman depends on

- The discrete logarithm problem.
- The Diffie-Hellman problem. Given g^a and g^b find g^{ab}.
- and more.

The ElGamal cryptosystem

Let $G = \langle g \rangle$. Alice's private key are the following: Private key: $a \in [1, |G|]$. Public key: g, g^a.

- To send a message $m \in G$ to Alice, Bob computes (g^r, mg^{ra}) for some arbitrary $r \in [1, |G|]$. Sends the ciphertext, i.e., the pair to Alice.
- To decrypt Alice computes g^{ar} from g^r and then g^{-ar} and then m from mg^{ar}.

The security of the ElGamal is equivalent to the Diffie-Hellman problem.

The MOR cryptosystem

Let G be a group and $\phi : G \to G$ be an automorphism; presented by the action of ϕ on some set of generators of G.

The keys

Secret key: a in $[1, |\phi|]$.

Public key: ϕ and ϕ^a.

To send a message $m \in G$

Ciphertext $(\phi^r, \phi^{ra}(m))$ for an arbitrary $r \in [1, |\phi|]$.

To decrypt

Use the secret key a to compute ϕ^{ra} and then ϕ^{-ra}, which gives us m.

Groups of order p^3, for an odd prime p

Classification of groups of order p^3

- There are two groups of order p^3, up to isomorphism.
- One of exponent p, and the other exponent p^2.
- For the rest of the talk we will talk about exponent p.

The group of exponent p, and order p^3 is given by

$$M := \langle x, y \mid x^p = 1 = y^p; [x, y] = z \in \mathsf{Z}(M); z^p = 1 \rangle$$

- M is an extra-special p-group; where the $M' = \Phi(M) = \mathsf{Z}(M) = \langle z \rangle$

Automorphisms of M

Two kinds of automorphisms

- One that is identity on the center. Forms a subgroup, denote it by H.
- Other that doesn't.

The one that is non-trivial on the center

$x \mapsto x$, $y \mapsto y^\theta$, where θ is primitive mod p.

Automorphism to matrices

$$\phi(x) = x^{m_1} y^{n_1} z^{l_1}$$
$$\phi(y) = x^{m_2} y^{n_2} z^{l_2}.$$

Then $[\phi(x), \phi(y)] = z^{\det(T)}$, where $T = \begin{pmatrix} m_1 & n_1 \\ m_2 & n_2 \end{pmatrix}$. This shows that $\det(T) \neq 0 \mod p$.

Automorphisms

Inner automorphisms I

$$x \mapsto xz^{d_x}$$
$$y \mapsto yz^{d_y}$$

An exact sequence

$$0 \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_p \longrightarrow \mathsf{Aut}(M) \longrightarrow \mathsf{GL}(2,p) \longrightarrow 1$$

Another exact sequence

$$0 \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_p \longrightarrow H \longrightarrow \mathsf{SL}(2,p) \longrightarrow 1$$

$$H/I \cong \mathsf{SL}(2,p)$$

The MOR cryptosystem on M

Recap

- We are given ϕ and ϕ^m, find m.

What about security? Nothing matters other than SL$(2,p)$!

- Corresponding to ϕ and ϕ^m, you can find matrices, A and A^m in GL$(2,p)$.
- Move to SL, it is better.
- In this case the DLP in $\langle\phi\rangle$ is the same as DLP in SL$(2,p)$.

The security of this cryptosystem

If the characteristic polynomial of the matrix corresponding to ϕ is irreducible, then the DLP in SL$(2,p)$ is the same as the DLP in $\mathbb{F}_{p^2}$.

Extra-special p group with exponent p

- Let P be the iterative central product of r Ms.
- Then P is an extra-special p group of order p^{2r+1}.

Bilinear form on P

Define $B : \frac{P}{\Phi(P)} \times \frac{P}{\Phi(P)} \to \mathbb{Z}_p$, as follows:

- For x, y in P, consider the image $\bar{x}, \bar{y}$ in $\frac{P}{\Phi(P)}$ and define $B(\bar{x}, \bar{y}) = c$ where $[x, y] = z^c$

B is a non-degenerate, skew-symmetric, bilinear form on $\frac{P}{\Phi(P)}$.

Generators and Relations of P

- $P = \langle x_1, \ldots, x_r, y_1, \ldots, y_r \mid [x_i, y_j] = 1, i \neq j;\ [x_i, y_i] = z \in \mathsf{Z}(P) \rangle$.
- Elements x_i, y_i, z are of order p

The automorphisms of P

Lemma

An automorphism of P preserves the bilinear form if and only if it trivial on the center $Z(P)$.

Proof.

$$[\phi(x), \phi(y)] = B\left(\phi(\bar{x}), \phi(\bar{y})\right) = B(\bar{x}, \bar{y}) = [x, y].$$ □

Two kinds of automorphisms

- That is trivial on $\mathsf{Z}(P)$, call it H.
- Other is of the form $x_i \mapsto x_i$ and $y_i \mapsto y_i^{\theta}$, where θ is primitive mod p.

$H/I \cong \mathsf{Sp}(2r, p)$.

The MOR cryptosystem

Like the previous case, the discrete logarithm problem in $\langle \phi \rangle$ is the same as the discrete logarithm problem in $\mathrm{Sp}(2r, p)$.

The security of this discrete logarithm problem in the same as the discrete logarithm problem in $\mathbb{F}_{p^{2r}}$.

So, what do we have?

- Computing the power of the automorphisms is at least as hard as computing the power of a matrix in $\mathrm{Sp}(2r, p)$.
- The discrete logarithm problem is as secure as the discrete logarithm problem in $\mathrm{Sp}(2r, p)$.
- Why not work in $\mathrm{Sp}(2r, p)$?