Constructing Public-Key Cryptographic Schemes based on Class Group Action on Set of Isogenous Elliptic Curves

Anton Stolbunov

CHiLE, 16. March 2009
Plan

— intro
— cryptographic schemes based on group action
— class group action on set of elliptic curves
— implementation details
— security of the schemes
Norwegian University of Science and Technology (NTNU)

— largest technological university in Norway
— located in Trondheim
— 7 faculties, 53 departments, 20 000 students
— information security research group with academics from departments of Telematics, Mathematics, Q2S, Electronics and Telecommunications
Motivation for the Research

— the security of current asymmetric cryptographic schemes is decreasing [RSA challenge], [Shor 95]
— cryptographic schemes based on new hard computational problems are needed
— elliptic curves and ideal class groups are well studied and good algorithms are available
CRYPTOGRAPHIC SCHEMES BASED ON GROUP ACTION
Semigroup Action on Set

$X$ is a set, $G$ is a finite commutative semigroup.

Left action of $G$ on $X$ is a map

$$G \times X \rightarrow X$$

$$(g, x) \mapsto g \ast x,$$

which satisfies the associativity property.

Example:

$X = \{3, 9, 5, 4\} \subset \mathbb{Z}/11\mathbb{Z}^\ast$, $G = \mathbb{Z}/5\mathbb{Z}^\ast$, $\ast$ is exponentiation.

<table>
<thead>
<tr>
<th>Elements of $G$</th>
<th>Permutations on $X$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(3)(9)(5)(4)</td>
</tr>
<tr>
<td>2</td>
<td>(3 9 4 5)</td>
</tr>
<tr>
<td>3</td>
<td>(3 5 4 9)</td>
</tr>
<tr>
<td>4</td>
<td>(3 4)(5 9)</td>
</tr>
</tbody>
</table>
Key Agreement Protocol based on Semigroup Action

Fix $x \in X$.

**Alice**

- $a \leftarrow^R G$
- $m_A \leftarrow a \ast x$

**Bob**

- $b \leftarrow^R G$
- $m_B \leftarrow b \ast x$

$k \leftarrow a \ast m_B$

$k \leftarrow b \ast m_A$

$a \ast m_B = a \ast (b \ast x) = (ab) \ast x = (ba) \ast x = b \ast (a \ast x) = b \ast m_A$
Public-Key Encryption based on Semigroup Action

$m \in \{0, 1\}^w$ is a message, $H = \{H_i : i \in I\}$ is a family of hash functions, where each $H_i$ is a function $X \rightarrow \{0, 1\}^w$.

\[ \mathcal{K}: \text{Key generation} \]
\[ \text{Input: -} \]
\[ \text{Output: } sk, pk \]
\[ sk \leftarrow R \rightarrow G \]
\[ r \leftarrow sk \ast x \]
\[ i \leftarrow R \rightarrow I \]
\[ pk \leftarrow (r, i) \]

\[ \mathcal{E}: \text{Encryption} \]
\[ \text{Input: } pk, m \]
\[ \text{Output: } ct \]
\[ a \leftarrow R \rightarrow G \]
\[ z \leftarrow a \ast r \]
\[ h \leftarrow H_i(z) \]
\[ y \leftarrow a \ast x \]
\[ c \leftarrow h \oplus m \]
\[ ct \leftarrow (c, y) \]

\[ \mathcal{D}: \text{Decryption} \]
\[ \text{Input: } sk, pk, ct \]
\[ \text{Output: } m \]
\[ z \leftarrow sk \ast y \]
\[ h \leftarrow H_i(z) \]
\[ m \leftarrow h \oplus c \]
CANDIDATE STRUCTURE: CLASS GROUP ACTION ON SET OF ELLIPTIC CURVES
Elliptic Curves over $\mathbb{C}$

For an elliptic curve $E/\mathbb{C}$, when $\mathbb{Z} \not\subseteq \text{End}(E)$, $E$ is said to have *complex multiplication*. In this case $\text{End}(E) \cong \mathcal{O}$, where $\mathcal{O}$ is an imaginary quadratic order.

For a maximal $\mathcal{O}_K$ define

$$\mathcal{ELL}(\mathcal{O}_K) = \left\{ \frac{E/\mathbb{C}}{\text{isomorphism over } \mathbb{C}} \middle| \text{End}(E) \cong \mathcal{O}_K \right\}.$$ 

$\mathcal{ELL}(\mathcal{O}_K)$ is a finite set.
Action of $\mathcal{CL}$ on $\mathcal{ELL}$

Let $\text{End}(E_\Lambda) \cong \mathcal{O}_K$. For an integral ideal $\alpha \subset \mathcal{O}_K$ we have that $\Lambda \subset \alpha^{-1}\Lambda$, and there is a natural homomorphism

$$\mathbb{C}/\Lambda \to \mathbb{C}/\alpha^{-1}\Lambda$$

$z \mapsto z$, which in turn induces a natural isogeny

$$\psi : E_\Lambda \to [\alpha] \ast E_\Lambda = E_{\alpha^{-1}\Lambda}$$

$\ker \psi$ is isomorphic to $\alpha^{-1}\Lambda/\Lambda \cong \mathcal{O}_K/\alpha$.

$\text{deg} \psi$ equals the norm $N(\alpha)$.

This $\mathcal{CL}(\mathcal{O}_K)$ action on $\mathcal{ELL}(\mathcal{O}_K)$ is free and transitive.
Elliptic Curves over $\mathbb{F}_p$

Reduction from $\mathbb{C}$ to $\mathbb{F}_p$: let $p \in \mathbb{Z}$ be a prime which splits in the Hilbert class field $H$ of $K$, and fix a prime ideal $\mathfrak{p} \subset \mathcal{O}_H$ lying above $p$.

The reduction of elliptic curves in $\mathcal{E}\mathcal{L}\mathcal{L}(\mathcal{O}_K)$ modulo $\mathfrak{p}$ preserves the endomorphism rings: $\text{End}_{\mathbb{F}_p}(\bar{E}) \simeq \mathcal{O}_K$. So we can define

$$\mathcal{E}\mathcal{L}\mathcal{L}_p,n(\mathcal{O}_K) = \left\{ E/\mathbb{F}_p \text{ with } \#E(\mathbb{F}_p) = n \text{ and } \text{End}(E) \simeq \mathcal{O}_K \right\}.$$  

The reduction modulo $\mathfrak{p}$ preserves the $\mathcal{C}\mathcal{L}(\mathcal{O}_K)$ action on $\mathcal{E}\mathcal{L}\mathcal{L}_p,n(\mathcal{O}_K)$.
Example of \( \mathcal{CL} \) Action on \( \mathcal{ELL}_{p,n} \)

\( E : y^2 = x^3 + x + 5 \) has 42 points over \( \mathbb{F}_{47} \), \( \Delta = -152 \) is fundamental and \( j_E = 27 \).

<table>
<thead>
<tr>
<th>( \mathcal{CL}(-152) )</th>
<th>Permutations on ( \mathcal{ELL}_{47,42}(-152) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( g = [(3, 2, \cdot)] )</td>
<td>( (27 19 41 24 15 12) )</td>
</tr>
<tr>
<td>( g^2 = [(6, 4, \cdot)] )</td>
<td>( (27 41 15)(19 24 12) )</td>
</tr>
<tr>
<td>( g^3 = [(2, 0, \cdot)] )</td>
<td>( (27 24)(19 15)(41 12) )</td>
</tr>
<tr>
<td>( g^4 = [(6, -4, \cdot)] )</td>
<td>( (27 15 41)(19 12 24) )</td>
</tr>
<tr>
<td>( g^5 = [(3, -2, \cdot)] )</td>
<td>( (27 12 15 24 41 19) )</td>
</tr>
<tr>
<td>( g^6 = [(1, 0, \cdot)] )</td>
<td>( (27)(19)(41)(24)(15)(12) )</td>
</tr>
</tbody>
</table>

Since \( (17, -16, \cdot) \in [(6, 4, \cdot)] \), there are isogenies of degree 17 defined over \( \mathbb{F}_{47} \).
IMPLEMENTATION DETAILS
Elements of $\mathcal{ELL}_{p,n}$

— represented by j-invariants of elliptic curves
— the equation of an elliptic curve belonging to the isomorphism class can also be stored
Elements of $\mathcal{CL}$

— fix a set of small primes

$$L = \left\{ \text{primes } l_i : \left( \frac{\Delta}{l_i} \right) = 1 \text{ and } l_i \leq l_{\text{max}} \right\},$$

where $l_{\text{max}} = c_0 (\log |\Delta|)^2$

— prime ideals $l_i = l_i \mathbb{Z} + \frac{b_i + \sqrt{\Delta}}{2} \mathbb{Z}$ of norms $N(l_i) = l_i$

— the ideals $l_i$ generate $\mathcal{CL}(\Delta)$ (under GRH)

— store elements of $\mathcal{CL}(\Delta)$ as vectors in $\mathbb{Z}^d$, $d = \#L$:

$$\mathbb{Z}^d \rightarrow \mathcal{CL}(\Delta)$$

$$(v_1, \ldots, v_d) \mapsto \prod_{i=1}^{d} [l_i]^{v_i}$$
Random Sampling from $\mathcal{CL}$

— suppose the class group structure is known:

$$\mathcal{CL}(\Delta) \simeq \bigotimes \langle [l_i] \rangle, \quad m_i = ord[l_i]$$

— choose a random vector $V = (v_1, \ldots, v_d)$, where $0 \leq v_i \leq m_i$. This gives the random element $\prod l_i^{v_i} \in \mathcal{CL}(\Delta)$

— reduce the vector $V$ modulo the lattice of relations among the ideal classes $[l_i]$ to get a shorter equivalent

— further speed optimisation of $V$
Non-Random Sampling from Large $\mathcal{CL}$

— the group structure can be computed with subexponential complexity $O(\exp \sqrt{2 \log \Delta \log \log \Delta})$ [Jacobson 99]. We were able to use up to 208-bit discriminants on a PC with 2Gb of RAM

— when the class group structure is unknown, one can implement a non-random sampling under the assumption that it is computationally indistinguishable from the random sampling
Implementing $\mathcal{CL}$ Action on $\mathcal{ELL}_{p,n}$

- compute $\prod_{i=1}^{d} l_i^{v_i} \ast E$ step-by-step by each factor
- on each step corresponding to a factor $l_i$, solve the modular equation $\Phi_{l_i}(x, j(E)) = 0$ in order to find the j-invariant of the next elliptic curve
- there are exactly two solutions, they correspond to the directions in isogeny cycles. It is possible to choose the necessary direction
Numerical Experiments

Intel x86-64 2GHz CPU (one core), Linux, PARI/GP. Average timing per one group action:

<table>
<thead>
<tr>
<th>$\log_2(# \mathcal{CL})$</th>
<th>$l_{\text{max}}$</th>
<th>$\mathcal{CL}$ structure</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>96</td>
<td>241</td>
<td>yes</td>
<td>1 m 24 s</td>
</tr>
<tr>
<td>128</td>
<td>271</td>
<td>no</td>
<td>1 m 49 s</td>
</tr>
<tr>
<td>160</td>
<td>277</td>
<td>no</td>
<td>3 m 23 s</td>
</tr>
<tr>
<td>256</td>
<td>499</td>
<td>no</td>
<td>1 h 20 m</td>
</tr>
</tbody>
</table>

Here $l_{\text{max}}$ is the maximal isogeny degree used.
SECURITY OF THE SCHEMES
Computational Problems

For a commutative semigroup $G$ acting on a set $X$.

**Computational Diffie-Hellman Semigroup Problem (CDHSP):**
given $x$, $y = a \ast x$ and $z = b \ast x$, find $(ab) \ast x$.

**Decisional Diffie-Hellman Semigroup Problem (DDHSP):**
given $x$, $y = a \ast x$, $z = b \ast x$ and $r$, decide if $r = (ab) \ast x$.

**Semigroup Action Problem (SAP):**
given $x$ and $y = a \ast x$, find $a$.

**Reducibility:**
can solve SAP $\implies$ can solve CDHSP $\implies$ can solve DDHSP
Complexity of Problem Instances with $CL$ action on $ELL_{p,n}$

**SAP:**
- most classic DLOG solvers cannot be adopted because for arbitrary $a, b \in ELL_{p,n}(\Delta)$ there is no efficient $a \cdot b$ operation
- using meet-in-the-middle technique: exponential time $O(\sqrt{h}((\ln h)^6 + (\ln h)^2))$, where $h = \#CL(\Delta)$ [Galbraith 99]
- class group structure is known: may use baby-step giant-step in a cyclic subgroup of $CL(\Delta)$. Still exponential time

**DDHSP** and **CDHSP** have not been considered in the literature.
Related Work

— our preliminary report [Stolbunov, Rostovtsev. IACR ePrint report 2006/145]

— independent research [Couveignes. IACR ePrint report 2006/291]

— computing the number of points on an elliptic curve [Schoof 85], [Elkies 98], [Atkin], [Morain 96]

— isogeny graphs [Kohel 96], [Galbraith 99], [Jao, Miller, Venkatesan 04]

— class group structure computation [Jacobson 99], [Hafner, McCurley 89]
Alternative Candidate Structure: Simple Semirings

Proposed in [Maze, Monico, Rosenthal 07].

Fix a simple semiring $R$. Example: $\{0, 1\}$ with max as addition and min as multiplication. Let $C$ be the center of $R$, and $n \in \mathbb{N}$.

For fixed $M_1, M_2 \in \text{Mat}_{n \times n}(R)$ define the action

$$(C[t] \times C[t]) \times \text{Mat}_{n \times n}(R) \rightarrow \text{Mat}_{n \times n}(R)$$

$$((p(t), q(t)), M) \mapsto p(M_1) \cdot M \cdot q(M_2).$$
Thank you!