Using semidirect product of (semi)groups in public key cryptography

Delaram Kahrobaei
City University of New York
Graduate Center: PhD Program in Computer Science
NYCCT: Mathematics Department

University of Wisconsin-Madison
June 15, 2016

The Diffie-Hellman public key exchange (1976)

1. Alice and Bob agree on a public (finite) cyclic group G and a generating element g in G. We will write the group G multiplicatively.
2. Alice picks a random natural number a and sends g^a to Bob.
3. Bob picks a random natural number b and sends g^b to Alice.
4. Alice computes $K_A = (g^b)^a = g^{ba}$.
5. Bob computes $K_B = (g^a)^b = g^{ab}$.

Since $ab = ba$ (because $\mathbb{Z}$ is commutative), both Alice and Bob are now in possession of the same group element $K = K_A = K_B$ which can serve as the shared secret key.

Security assumptions

To recover g^{ab} from (g, g^a, g^b) is hard.

To recover a from (g, g^a) (discrete log problem) is hard.

Variations on Diffie-Hellman: why not just multiply them?

1. Alice and Bob agree on a (finite) cyclic group G and a generating element g in G. We will write the group G multiplicatively.
2. Alice picks a random natural number a and sends g^a to Bob.
3. Bob picks a random natural number b and sends g^b to Alice.
4. Alice computes $K_A = (g^b) \cdot (g^a) = g^{b+a}$.
5. Bob computes $K_B = (g^a) \cdot (g^b) = g^{a+b}$.

Obviously, $K_A = K_B = K$, which can serve as the shared secret key.
Drawback: anybody can obtain K the same way!

Semidirect product

Let G, H be two groups, let $Aut(G)$ be the group of automorphisms of G, and let $\rho : H \to Aut(G)$ be a homomorphism. Then the semidirect product of G and H is the set

$$\Gamma = G \rtimes_\rho H = \{(g, h) : g \in G,\ h \in H\}$$

with the group operation given by

$$(g, h)(g', h') = (g^{\rho(h')} \cdot g',\ h \cdot h').$$

Here $g^{\rho(h')}$ denotes the image of g under the automorphism $\rho(h')$.

Extensions by automorphisms

If $H = Aut(G)$, then the corresponding semidirect product is called the *holomorph* of the group G. Thus, the holomorph of G, usually denoted by $Hol(G)$, is the set of all pairs $(g,\ \phi)$, where $g \in G,\ \phi \in Aut(G)$, with the group operation given by

$$(g,\ \phi) \cdot (g',\ \phi') = (\phi'(g) \cdot g',\ \phi \cdot \phi').$$

It is often more practical to use a subgroup of $Aut(G)$ in this construction.

Also, if we want the result to be just a semigroup, not necessarily a group, we can consider the semigroup $End(G)$ instead of the group $Aut(G)$ in this construction.

Key exchange using extensions by automorphisms (Habeeb-Kahrobaei-Koupparis-Shpilrain)

- Let G be a group (or a semigroup).
- An element $g \in G$ is chosen and made public as well as an arbitrary automorphism (or an endomorphism) ϕ of G.
- Bob chooses a private $n \in \mathbb{N}$.
- While Alice chooses a private $m \in \mathbb{N}$.
- Both Alice and Bob are going to work with elements of the form (g, ϕ^k), where $g \in G,\ k \in \mathbb{N}$.

Using semidirect product (cont.)

1. Alice computes

$$(g, \phi)^m = (\phi^{m-1}(g) \cdots \phi^2(g) \cdot \phi(g) \cdot g,\ \phi^m)$$

and sends **only the first component** of this pair to Bob. Thus, she sends to Bob **only** the element

$$a = \phi^{m-1}(g) \cdots \phi^2(g) \cdot \phi(g) \cdot g$$

of the group G.

2. Bob computes

$$(g, \phi)^n = (\phi^{n-1}(g) \cdots \phi^2(g) \cdot \phi(g) \cdot g,\ \phi^n)$$

and sends **only the first component** of this pair to Alice:

$$b = \phi^{n-1}(g) \cdots \phi^2(g) \cdot \phi(g) \cdot g.$$

Using semidirect product (cont.)

3. Alice computes

$$(b, x) \cdot (a,\ \phi^m) = (\phi^m(b) \cdot a,\ x \cdot \phi^m).$$

Her key is now

$$K_A = \phi^m(b) \cdot a.$$

Note that she does not actually "compute" $x \cdot \phi^m$ because she does not know the automorphism x; recall that it was not transmitted to her. But she does not need it to compute K_A.

Using semidirect product (cont.)

4. Bob computes

$$(a, y) \cdot (b,\ \phi^n) = (\phi^n(a) \cdot b,\ y \cdot \phi^n).$$

His key is now

$$K_B = \phi^n(a) \cdot b.$$

Again, Bob does not actually "compute" $y \cdot \phi^n$ because he does not know the automorphism y.

5. Since

$$(b, x) \cdot (a,\ \phi^m) = (a,\ y) \cdot (b,\ \phi^n) = (g,\ \phi)^{m+n},$$

we should have $K_A = K_B = K$, the shared secret key.

Special case: Diffie-Hellman

$G = \mathbb{Z}_p^*$
$\phi(g) = g^k$ for all $g \in G$ and a fixed k, $1 < k < p-1$, where k is relatively prime to $p-1$.

Then $(g, \phi)^m = (\phi^{m-1}(g) \cdots \phi(g) \cdot \phi^2(g) \cdot g,\ \phi^m)$.
The first component is equal to $g^{k^{m-1}+\ldots+k+1} = g^{\frac{k^m-1}{k-1}}$.
The shared key $K = g^{\frac{k^{m+n}-1}{k-1}}$.

Special case: Diffie-Hellman

"The Diffie-Hellman type problem" would be to recover the shared key

$$K = g^{\frac{k^{m+n}-1}{k-1}}$$

from the triple

$$(g,\ g^{\frac{k^m-1}{k-1}},\ g^{\frac{k^n-1}{k-1}}).$$

Since g and k are public, this is equivalent to recovering $g^{k^{m+n}}$ from the triple $(g,\ g^{k^m},\ g^{k^n})$, i.e., this is exactly the standard Diffie-Hellman problem.

Group ring

Definition (Group ring)

Let G be a group written multiplicatively and let R be any commutative ring with nonzero unity. The group ring $R[G]$ is defined to be the set of all formal sums

$$\sum_{g_i \in G} r_i g_i$$

where $r_i \in R$, and all but a finite number of r_i are zero.

We define the sum of two elements in RG by

$$\left(\sum_{g_i \in G} a_i g_i\right) + \left(\sum_{g_i \in G} b_i g_i\right) = \sum_{g_i \in G} (a_i + b_i) g_i.$$

Note that $(a_i + b_i) = 0$ for all but a finite number of i, hence the above sum is in $R[G]$. Thus $(R[G], +)$ is an abelian group. Multiplication of two elements of $R[G]$ is defined by the use of the multiplications in G and R as follows:

$$\left(\sum_{g_i \in G} a_i g_i\right)\left(\sum_{g_i \in G} b_i g_i\right) = \sum_{g_i \in G} \left(\sum_{g_j g_k = g_i} a_j b_k\right) g_i.$$

Platform: matrices over group rings

- Our general protocol can be used with *any* non-commutative group G if ϕ is selected to be an inner automorphism.
- Furthermore, it can be used with any non-commutative *semigroup* G as well, as long as G has some invertible elements; these can be used to produce inner automorphisms.
- A typical example of such a semigroup would be a semigroup of matrices over some ring.

Platform: matrices over group rings

We use the semigroup of 3×3 matrices over the group ring $\mathbb{Z}_7[A_5]$, where A_5 is the alternating group on 5 elements. Then the public key consists of two matrices: the (invertible) conjugating matrix H and a (non-invertible) matrix M. The shared secret key then is:

$$K = H^{-(m+n)}(HM)^{m+n}.$$

Here we use an extension of the semigroup G by an inner automorphism φ_H, which is conjugation by a matrix $H \in GL_3(\mathbb{Z}_7[A_5])$. Thus, for any matrix $M \in G$ and for any integer $k \geq 1$, we have

$$\varphi_H(M) = H^{-1}MH;\ \varphi_H^k(M) = H^{-k}MH^k.$$

1. Alice and Bob agree on public matrices $M \in G$ and $H \in GL_3(\mathbb{Z}_7[A_5])$. Alice selects a private positive integer m, and Bob selects a private positive integer n.

2. Alice computes $(M, \varphi_H)^m = (H^{-m+1}MH^{m-1} \cdots H^{-2}MH^2 \cdot H^{-1}MH \cdot M,\ \varphi_H^m)$ and sends **only the first component** of this pair to Bob. Thus, she sends to Bob **only** the matrix

$$A = H^{-m+1}MH^{m-1} \cdots H^{-2}MH^2 \cdot H^{-1}MH \cdot M = H^{-m}(HM)^m.$$

3. Bob computes
$(M, \varphi_H)^n = (H^{-n+1}MH^{n-1} \dots H^{-2}MH^2 \cdot H^{-1}MH \cdot M,\ \varphi_H^n)$
and sends **only the first component** of this pair to Alice.
Thus, he sends to Alice **only** the matrix

$$B = H^{-n+1}MH^{n-1} \dots H^{-2}MH^2 \cdot H^{-1}MH \cdot M = H^{-n}(HM)^n.$$

4. Alice computes $(B, x) \cdot (A,\ \varphi_H^m) = (\varphi_H^m(B) \cdot A,\ x \cdot \varphi_H^m)$. Her key is now $K_{Alice} = \varphi_H^m(B) \cdot A = H^{-(m+n)}(HM)^{m+n}$. Note that she does not actually "compute" $x \cdot \varphi_H^m$ because she does not know the automorphism $x = \varphi_H^n$; recall that it was not transmitted to her. But she does not need it to compute K_{Alice}.

5. Bob computes $(A, y) \cdot (B,\ \varphi_H^n) = (\varphi_H^n(A) \cdot B,\ y \cdot \varphi_H^n)$. His key is now $K_{Bob} = \varphi_H^n(A) \cdot B$. Again, Bob does not actually "compute" $y \cdot \varphi_H^n$ because he does not know the automorphism $y = \varphi_H^m$.

6. Since $(B, x) \cdot (A,\ \varphi_H^m) = (A,\ y) \cdot (B,\ \varphi_H^n) = (M,\ \varphi_H)^{m+n}$, we should have $K_{Alice} = K_{Bob} = K$, the shared secret key.

Security assumptions

To recover $H^{-(m+n)}(HM)^{m+n}$ from $(M,\ H,\ H^{-m}(HM)^m,\ H^{-n}(HM)^n)$ is hard.

To recover m from $H^{-m}(HM)^m$ is hard.

Nilpotent groups and p-groups

Definition

First we recall that a *free group* F_r on $x_1, \ldots, x_r$ is the set of *reduced words* in the alphabet $\{x_1, \ldots, x_r, x_1^{-1}, \ldots, x_r^{-1}\}$.

- It is a fact that every group that can be generated by r elements is the factor group of F_r by an appropriate normal subgroup. We are now going to define two special normal subgroups of F_r.
- The normal subgroup F_r^p is generated (as a group) by all elements of the form g^p, $g \in F_r$. In the factor group F_r/F_r^p every nontrivial element therefore has order p (if p is a prime).

Nilpotent groups and p-groups (cont.)

- The other normal subgroup that we need is somewhat less straightforward to define. Let $[a, b]$ denote $a^{-1}b^{-1}ab$. Then, inductively, let $[y_1, \ldots, y_{c+1}]$ denote $[[y_1, \ldots, y_c], y_{c+1}]$. For a group G, denote by $\gamma_c(G)$ the (normal) subgroup of G generated (as a group) by all elements of the form $[y_1, \ldots, y_c]$. If $\gamma_{c+1}(G) = \{1\}$, we say that the group G is nilpotent of nilpotency class c.
- The factor group $F_r/\gamma_{c+1}(F_r)$ is called *the free nilpotent group* of nilpotency class c. This group is infinite.

Free nilpotent p-group

- The group $G = F_r/F_r^{p^2} \cdot \gamma_{c+1}(F_r)$ is what we suggest to use as the platform for the key exchange protocol.
- This group, being a nilpotent p-group, is finite. Its order depends on p, c, and r. For efficiency reasons, it seems better to keep c and r fairly small (in particular, we suggest $c = 2$ or 3), while p should be large enough to make the dimension of linear representations of G so large that a linear algebra attack would be infeasible.
- The minimal faithful representation of a finite p-group as a group of matrices over a finite field of characteristic p is in this case of dimension $1 + p$. Thus, if p is, say, a 100-bit number, a linear algebra attack is already infeasible.

Thanks

Thank You!