Presented at Asiacrypt 2004

On the Security of MOR Public Key Cryptosystem

2004. 12. 8.

In-Sok Lee, Woo-Hwan Kim, Daesung Kwon, Sangil Nahm, Nam-Seok Kwak, Yoo-Jin Baek

Information Security and Cryptology Research Center
Seoul National University

Contents

- MOR Public Key Cryptosystem
  - Related Problems
- Security Analysis
  - Generic Complexity
  - Central Commutator Attack
  - Group Extensions
- Conclusion

MOR Public Key Cryptosystem

- Crypto 2001,
  S. Paeng, K. Ha, J. Kim and S. Chee,
  "New public key cryptosystem
  using finite non-abelian groups"

- MOR = more, morphism, ……?
  - more security
  - more speed
  - easier signature scheme ……

Current Status of MOR

- All the suggested groups were unsatisfactory.
  - Paeng et al., Cryptology ePrint Archive, 2001.
  - Paeng, Inf. Process. Lett., 2003.
  - Tobias, Proc. PKC, 2003.

- Waiting for a suggestion ;
  - *"good"* candidates of finite groups G,
  - security parameters ; $|G|$, $|Z(G)|$, $|\mathrm{Inn}(g)|$, ……

Our Objective

- We are not trying to suggest a new candidate.
- We rather intend to reveal the reason why it is not easy to find a "*good*" candidate.

Standard Notations

- For $g \in G$, define $\mathrm{Inn}(g) \in \mathrm{Aut}(G)$ by
$$\mathrm{Inn}(g)(h) = g^{-1}hg, \quad (h \in G)$$
- Inner automorphism group ;
$$\mathrm{Inn}(G) = \{\ \mathrm{Inn}(g) \mid g \in G\ \} \leq \mathrm{Aut}(G)$$
- Center of G ;
$$Z(G) = \{\ z \in G \mid gz = zg \text{ for all } g \in G\ \}$$
- $\mathrm{Inn}(G) \approx G / Z(G)$
- $\overline{g}$ = [image of g in $G / Z(G)$]
- $|g|$ = [order of g in G]

MOR Public Key Cryptosystem

Setup	G : finite non-abelian group $\{\gamma_i \mid i \in \boldsymbol{I}\}$; generators of G	
Public Key	$\mathrm{Inn}(g)$ and $\mathrm{Inn}(g^s)$	$\{\mathrm{Inn}(g)(\gamma_i) \mid i \in \boldsymbol{I}\}$ $\{\mathrm{Inn}(g^s)(\gamma_i) \mid i \in \boldsymbol{I}\}$
Secret Key	$s \in \mathbb{N}$	$s \pmod{\lvert\mathrm{Inn}(g)\rvert}$
Encryption	$a \in_R \mathbb{N}$, compute $E = (\mathrm{Inn}(g^s))^a\,(m)$ and $\psi = \mathrm{Inn}(g^a)$	message : $m \in G$ ciphertext : (E, ψ)
Decryption	$\psi^{-s}(E) = m$	

Related Problems

- Special Conjugacy Problem(SCP) :
  - Given $\phi = \mathrm{Inn}(g)$, find g_1 such that $\phi = \mathrm{Inn}(g_1)$.
  - That is, given $\{\mathrm{Inn}(g)(\gamma_i) \mid i \in \boldsymbol{I}\}$, find g_1 such that

$$\mathrm{Inn}(g_1)(\gamma_i) = \mathrm{Inn}(g)(\gamma_i) \quad \text{for all } i \in \boldsymbol{I}.$$

- Assume SCP is easy for G.
  - Otherwise, ……

Related Problems

- $MOR(G) = DLP(Inn(G))$:
  Given $\phi = Inn(g)$ and $\phi^s = Inn(g^s)$, find s.

- Assuming SCP is easy for G
  - Find g_1 and g_2 such that $Inn(g_1) = \phi$ and $Inn(g_2) = \phi^s$.
  - Then, $g_2 z = g_1^s$ for some $z \in Z(G)$.

- Solve DLP over G :
  - For each z in $Z(G)$, try to solve $DLP(g_1, g_2 z)$.

  - If $|Z(G)|$ is small, $MOR(G)$ is similar to $DLP(G)$.
  - If $|Z(G)|$ is sufficiently large, $MOR(G)$ might be difficult enough, even though $DLP(G)$ is easy……(?)

Related Problems

- (Assume SCP is easy for G.)

  Given g_1 and g_2 such that $g_2 z = g_1^s$ for some $z \in Z(G)$, find s,

  i.e., given g_1 and g_2 such that $\overline{g_2} = \overline{g_1}^s$, find s.

- Note that s is determined up to $(\mathrm{mod}\ |\overline{g}|)$

- Thus,

  $$\mathrm{MOR}(G) = \mathrm{DLP}(\mathrm{Inn}(G)) = \mathrm{DLP}(G/Z(G)).$$

Generic Complexity

- Generic algorithm for DLP
  - Algorithm which does not exploit any particular properties of representations of the group is called generic.
  - Examples ;
    - Baby-step giant-step
    - Pollard rho method
    - Pohlig-Hellman algorithm

Generic Complexity

- Group operations of $G/Z(G)$ can be realized using group operations of G.
  - Group multiplication ; $\mathrm{Mul}_{G/Z}(g_1,g_2) = \mathrm{Mul}_G(g_1,g_2)$
  - Inversion ; $\mathrm{Inv}_{G/Z}(g) = \mathrm{Inv}_G(g)$
  - Equality test ;
    $\mathrm{Equ}_{G/Z}(g_1,g_2)$ =True, if $g_1g_2^{-1}\gamma_i = \gamma_i g_1g_2^{-1}$ for all $i \in \boldsymbol{I}$,
    False, otherwise

Information Security and Cryptology Research Center
SEOUL NATIONAL UNIVERSITY

Generic Complexity ; Pohlig-Hellman

- May assume ;
  $|\boldsymbol{I}|$ = the number of given generators in G
  $= O(\log |G|)$

- Only need $O(\log |G|)$ equality tests in G, not $|Z(G)|$ equality tests in G.

- $DLP(G/Z(G))$ is $O(\log|G|)$ times more difficult than $DLP(G)$ in a generic sense.

Information Security and Cryptology
Research Center
SEOUL NATIONAL UNIVERSITY

Central Commutator Attack

- $(\mathrm{Inn}(g), \mathrm{Inn}(g^s)) = (\phi, \phi^s)$ is given.
- Suppose we can find $h, z \in G$ such that
  - $z = \phi(h^{-1})h = g^{-1}h^{-1}gh \neq 1$
  - $\phi(z^{-1})z = 1$ (i.e. z and g commute).
  - Then z^s can be computed from ϕ^s ;

$$\phi^s(h^{-1})h = g^{-s}h^{-1}g^s h = g^{-s}(h^{-1}gh)^s = g^{-s}(gz)^s = z^s.$$

- Reduction from $\mathrm{DLP}(\mathrm{Inn}(G))$ to $\mathrm{DLP}(G)$
  - Compute (z, z^s) from (ϕ, ϕ^s).
  - Solve $\mathrm{DLP}(G)$.

Information Security and Cryptology Research Center
SEOUL NATIONAL UNIVERSITY

Central Commutator Attack

- Assume G is nilpotent
  - $G=G^0>G^1>\cdots>G^{k-1}>G^k=1$, where $G^i=[G,G^{i-1}]$
  - $G^{k-1}\subset Z(G)$ and $G^{k-2}\not\subset Z(G)$
  - Get $h\in G^{k-2}\setminus Z(G)$
  - Put $z=g^{-1}h^{-1}gh\in Z(G)$
  - "Central commutators" (z, z^s)

  - How to find h ?
  - $z\neq 1$ is not guaranteed

Central Commutator Attack

- Algorithm (when G is nilpotent)

Algorithm-1	
Input	$\phi = \mathrm{Inn}(g)$, ϕ^s
Step 1	Put $\sigma(x) = \phi(x^{-1})x = g^{-1}x^{-1}gx$ Choose x_0 such that $\sigma(x_0) \neq 1$, i.e., $\phi(x_0) \neq x_0$
Step 2	Put $x_m = \sigma(x_{m-1})$ n ; the smallest integer such that $x_n = 1$
Step 3	Put $h=x_{n-2}$, $z=x_{n-1}$ and compute $z^s = \phi^s(h^{-1})h$
Output	Get z, z^s with $z \neq 1$

- Solving DLP(z, z^s) over G, we can find s (mod $|z|$).

Central Commutator Attack

- Next, apply Pohlig-Hellman algorithm ;
  - Put $|\phi| = m = \prod p_i^{e_i}$
  - Compute $s \pmod{p_i^{e_i}}$ for each i.
    - Suppose $m = p^e$ and $s \pmod{p^e} = \sum s_r p^r$
    - Put $\psi = \phi^{m/p}$ and $\psi_0 = (\phi^s)^{m/p}$
    - Applying Algorithm-1 to (ψ, ψ_0), get h, z, z^{s_0} $(|z|=p)$
    - Compute $s_0 \pmod{p}$
    - Computing $s_r \pmod{p}$ inductively, get $s \pmod{p^e}$
  - Using CRT, completely recover $s \pmod{m}$
- Central commutator attack is 'generic'.

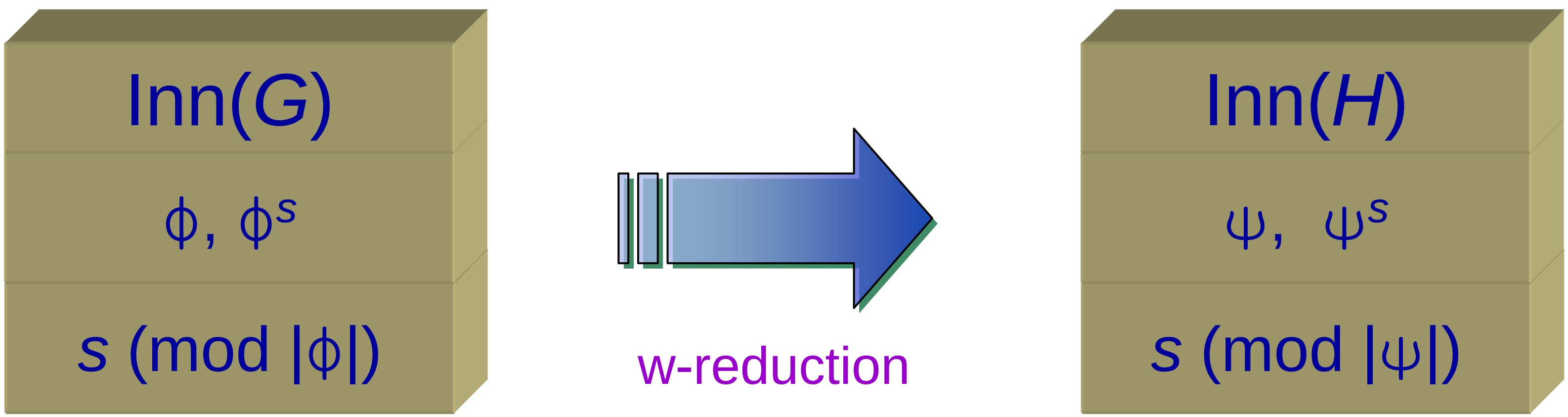
Central Commutator Attack

- G is *'nearly'* nilpotent
  iff $G/Z(G)$ has non-trivial center
  iff G has non-trivial upper central series

- Then, central commutator attack works.
  - $\exists\, x \in G \setminus Z(G)$ such that $z = x^{-1}y^{-1}xy \in Z(G)$ for all $y \in G$

Weak-Reduction

- Definition (w-reduction)
  - $H \lhd G$

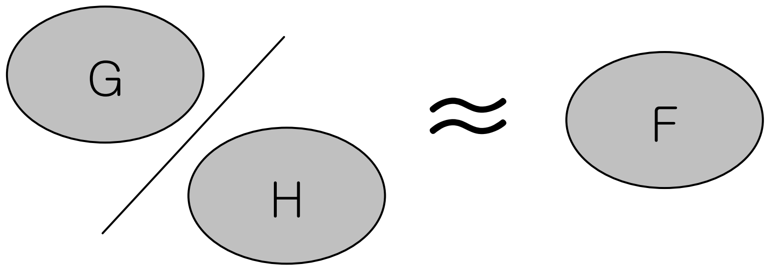


  - $s \pmod{|\psi|}$ gives partial information on $s \pmod{|\phi|}$.

Group Extensions

- If $H \lhd G$ and $G / H \approx F$,
  G is called a group extension of H by F
- Well-known facts ;
  - If G is a group extension of H by F,
    there exist $T : F \to \mathrm{Aut}(H)$ and $f : F \times F \to \mathrm{H}$ such that
    - $T(\tau) \circ T(\sigma) = \mathrm{Inn}(f(\sigma,\tau)) \circ T(\sigma\tau)$
    - $f(\sigma,\tau\rho)\, f(\tau,\rho) = f(\sigma\tau,\rho)\, T(\rho)(f(\sigma,\tau))$
    - $f(1,1)=1$.
- $G = [H, F, T, f]$; group extension data

Group Extensions



- Assume group extension data $G = [H, F, T, f\,]$ is known.
- Theorem ;
  - When F is non-abelian,
    DLP(Inn(G)) can be w-reduced to DLP(Inn(F)).
  - When $F = \mathbb{Z}_p$,
    DLP(Inn(G)) can be w-reduced to DLP(Inn(H)).

Group Extensions

- Every finite group G has a composition series.
- May regard G as a group extended by finite simple groups for finitely many times.
- G may have many maximal normal subgroups.

Group Extensions

- When $F = \mathbb{Z}_p$,
- Case 1 ; $G\,/\,Z(G) \approx H\,/\,Z(H)$
  - $|Z(G)| > |Z(H)|$
  - The above isomorphism is computable.
  - MOR(G) is completely reduced to MOR(H).
  - E.g., $G = SL_2(p) \times_{\theta} \mathbb{Z}_p$, (semi-direct product)
- Case 2 ; $|Z(G)| \leq |Z(H)|$
  - MOR(G) can be w-reduced to MOR(H).

Group Extensions ; Conclusion

- To find a *'good'* candidate G for MOR system, it is better to conceal the information on
  - (maximal) normal subgroups,
  - group extension data,
  - composition series,
  - lower / upper central series,
  - etc……

Conclusion

- Security of MOR system
  - Based on DLP(Inn(G)) = DLP(G/ Z(G))
  - In a generic sense,

    [complexity of DLP(Inn(G))]

    = O(log |G|) x [complexity of DLP(G)]

- Central commutator attack
  - If G is nilpotent,

    DLP(Inn(G)) can be completely reduced to DLP(G)
  - If G is '*nearly*' nilpotent ......

Conclusion

- Group extensions
  - If G is a group extension of H by $\mathbb{Z}_p$, $MOR(G)$ can be w-reduced to $MOR(H)$.

- Remark : Discrete Log Problem depends not only on the algebraic structure of G, but on the (re)presentation of G.