A glimpse into MOR cryptosystem

Ayan Mahalanobis Anupam Singh
Sushil Bhunia Pralhad Shinde

IISER Pune

04 June 2019

Why study MOR cryptosystem?

Quantum Computers

With the quantum computers becoming a reality, one should look for new cryptosystems. The MOR cryptosystem offers a new way to construct cryptosystems out of algebraic structures.

Why study MOR cryptosystem?

Quantum Computers

With the quantum computers becoming a reality, one should look for new cryptosystems. The MOR cryptosystem offers a new way to construct cryptosystems out of algebraic structures.

Application of algebra

The MOR cryptosystem can offer us nice problems to solve. In particular while working with the MOR cryptosystem over classical groups we found a Gaussian elimination algorithm in orthogonal, symplectic and unitary groups.

What is a MOR cryptosystem?

It is a simple generalization of the classic ElGamal cryptosystem. In case of the MOR cryptosystem, we work with the automorphism group of a algebraic structure. The discrte logarithm problem works in the automorphism group not the group.

What is a MOR cryptosystem?

It is a simple generalization of the classic ElGamal cryptosystem. In case of the MOR cryptosystem, we work with the automorphism group of a algebraic structure. The discrte logarithm problem works in the automorphism group not the group.

Though the square root attacks on the discrete logarithm problem will still work. However, this way might produce discrete logarithm problems that are resistant to quantum attacks.

Description of the MOR cryptosystem

Let G be a finite group and ϕ an automorphism of that group. The group G is generated by $\{g_1, g_2, \ldots, g_s\}$.

Public key

Automorphisms ϕ and ϕ^m. These automorphisms are presented as action on generators $\{\phi(g_i)\}_{i=1}^{s}$ and $\{\phi^m(g_i)\}_{i=1}^{s}$.

Description of the MOR cryptosystem

Let G be a finite group and ϕ an automorphism of that group. The group G is generated by $\{g_1, g_2, \ldots, g_s\}$.

Public key

Automorphisms ϕ and ϕ^m. These automorphisms are presented as action on generators $\{\phi(g_i)\}_{i=1}^{s}$ and $\{\phi^m(g_i)\}_{i=1}^{s}$.

Private key

m.

Description of the MOR cryptosystem

Let G be a finite group and ϕ an automorphism of that group. The group G is generated by $\{g_1, g_2, \ldots, g_s\}$.

Public key

Automorphisms ϕ and ϕ^m. These automorphisms are presented as action on generators $\{\phi(g_i)\}_{i=1}^{s}$ and $\{\phi^m(g_i)\}_{i=1}^{s}$.

Private key

m.

Encryption

To encrypt a message $g \in G$, choose random r and compute $(\phi^r, \phi^{rm}(g))$.

Description of the MOR cryptosystem

Let G be a finite group and ϕ an automorphism of that group. The group G is generated by $\{g_1, g_2, \ldots, g_s\}$.

Public key

Automorphisms ϕ and ϕ^m. These automorphisms are presented as action on generators $\{\phi(g_i)\}_{i=1}^{s}$ and $\{\phi^m(g_i)\}_{i=1}^{s}$.

Private key

m.

Encryption

To encrypt a message $g \in G$, choose random r and compute $(\phi^r, \phi^{rm}(g))$.

Decryption

Use m to compute ϕ^{mr} from ϕ^r and then $\phi^{-mr}\left(\phi^{mr}(g)\right) = g$.

Issues with a MOR cryptosystem

There are two major issues with any MOR cryptosystem.

1. The number of generators. Bigger the number of generators larger the key size.
2. Solving the word problem in those generators.

What is the right group for a MOR cryptosystem

Two extremes in finite groups.

A. Finite p-groups.

B. Finite simple groups.

The situation with finite p-groups

The situation with finite p-groups is somewhat resolved. For the purpose of MOR cryptosystem there are two kinds of automorphisms – p-automorphisms whose order is a power of p and p'-automorphism whose order is co-prime to p.

For p'-automorphism ϕ; look at the action of ϕ on the Frattini quotient. This reduces the DLP in ϕ to a DLP in matrices over $\mathbb{Z}_p$ of size of the cardinality of the minimal generating set.

For p-automorphism there is no such known reduction.

The case of MOR cryptosystem with split orthogonal groups

Automorphisms

Diagonal automorphisms.

Inner automorphisms.

Central automorphisms.

Field automorphisms.

Graph automorphisms

The case of MOR cryptosystem with split orthogonal groups

Automorphisms

Diagonal automorphisms.

Inner automorphisms.

Central automorphisms.

Field automorphisms.

Graph automorphisms

We only concentrate on the inner automorphisms.

Generators for the split orthogonal group

$O^+(d, q)$ where $d = 2l$

$$
\begin{aligned}
x_{i,j}(t) &= I + t(e_{i,j} - e_{-j,-i}) && i \neq j && (1)\\
x_{i,-j}(t) &= I + t(e_{i,-j} - e_{j,-i}) && i < j && (2)\\
x_{-i,j}(t) &= I + t(e_{-i,j} - e_{-j,i}) && i < j && (3)\\
w_i &= I - e_{i,i} - e_{-i,-i} + e_{i,-i} + e_{-i,i} && i \leq i \leq l && (4)
\end{aligned}
$$

Security of the MOR cryptosystem on split orthogonal groups

The group is the split orthogonal group.

The automorphism is the inner automorphism.

The generators are the Chevalley generators.

Security of the MOR cryptosystem on split orthogonal groups

The group is the split orthogonal group.

The automorphism is the inner automorphism.

The generators are the Chevalley generators.

The security can be either $\mathbb{F}_{q^d}$ or $\mathbb{F}_{q^{d^2}}$. It depends on whether one can find the conjugating element that defines the automorphism or not.
In the case of the orthogonal group, it seems like that the security is that of $\mathbb{F}_{q^{d^2}}$.

Conclusions

Why study MOR cryptosystem?

Conclusions

Why study MOR cryptosystem?

While studying the MOR cryptosystem we developed a Gaussian elimination algorithm for the symplectic, orthogonal and unitary groups.

Conclusions

Why study MOR cryptosystem?

While studying the MOR cryptosystem we developed a Gaussian elimination algorithm for the symplectic, orthogonal and unitary groups.

Majority of this talk is from the recent publication:
The MOR cryptosystem in classical groups with a Gaussian elimination algorithm for symplectic and orthogonal groups published as a book chapter by IntechOpen.