Public key cryptography based on non-invertible matrices

Georgi Guninski*

April 13, 2022

Initial revision: Sat 02 Apr 2022

Abstract

We present public key cryptography algorithm based on non-ivertible matrices. Experimental data suggests the algorithm is not ready for usage, but the idea has the potential to be improved.

There was discussion on mathoverflow.net [2] [3] in the end of March 2022.

1 Algorithm guninski2 for public key cryptography based on non-invertible matrices

Alice and Bob agree on a prime p and positive integer n

Working over $\mathbb{F}_p$ and all matrices are square $n \times n$.

Alice chooses invertible matrix X_A and non-invertible matrix M_A and makes public $P_A = X_A M_A$.

Bob chooses invertible matrix X_B and non-invertible matrix M_B and makes public $P_B = M_B X_B$.

Alice makes public $S_A = M_A P_B = M_A M_B X_B$.

Bob makes public $S_B = P_A M_B = X_A M_A M_B$.

To compute the shared secret $S = M_A M_B$, Allice compute $S = X_A^{-1} S_B = X_A^{-1} X_A M_A M_B = M_A M_B$ and Bob computes $S = S_A X_B^{-1} = M_A M_B X_B X_B^{-1} = M_A M_B$

At this point, everyone knows P_A, P_B, S_A, S_B and only Alice and Bob know the shared secret $S = M_A M_B$.

Observe that P_A, P_B, S_A, S_B are non-invertible, that is they are singular with determinants zero.

If P_B were invertible, an adversary could break the system by computing $S_A P_B^{-1} = M_A P_B P_B^{-1} = M_A$.

Let $I(P_A, P_B, S_A, S_B)$ be the set of pseudo keys, that is the set of quadruples (X'_A, M'_A, X'_B, M'_B) satisfying the construction of the algorithm:

$$P_A = X'_A M'_A \qquad (1)$$

$$P_B = M'_B X'_B \qquad (2)$$

*email gguninski@gmail.com,email guninski@guninski.com

$$S_A = M'_A P_B \qquad (3)$$
$$S_B = P_A M'_B \qquad (4)$$

.

Define good key to be a pseudo key, which recovers the shared secret $M_A M_B$.

Trivially the good keys are in the set I, but I have many other members, which are not good.

Observe that $(1), (3)$ depend only on X'_A, M'_A and $(2), (4)$ dependent only on X'_B, M'_B.

Let S_A be the set of pairs of matrices satisfying $(1), (3)$.

Let S_B be the set of pairs of matrices satisfying $(2), (4)$.

We have

$$I(P_A, P_B, S_A, S_B) = \{(X'_A, M'_A, X'_B, M'_B) : X'_A, M'_A \in S_A, X'_B M'_B \in S_B\}$$

Observe that for $X'_A, M'_A \in S_A$ all of members of S_B give pseudo key.

2 Algebraic attack

Given P_A, P_B, S_A, S_B, the goal is to find the shared secret $M_A M_B$.

Take four matrices with entries variables: X'_A, M'_A, X'_B, M'_B.

Substitute in the construction to get four matrix equations.

Equating the entries in the equations, we get $4n^2$ equations with $4n^2$ variables.

Two of the matrix equations $(3), (4)$ are the form constant matrix times unknown matrix, which gives $2n^2$ linear equations. Using gaussian elimination, eliminate the linear variables and substitute in the other two equations $(1), (2)$, leading to only $2n^2$ quadratic equations.

The solutions of these equations are the pseudo keys.

3 Experimental data

We tried purely experimental approach to find the sets of pseudo keys and the good pseudo keys using sagemath [1].

Modulo errors, we tried small p, n using our implementation.

$p = 11, n = 2$ pseudo keys= 12321 good keys= 221 $|S_A| = 111, |S_B| = 111, |S_A * S_B| = 12321$

$p = 2, n = 4$ pseudo keys= 1404 good keys= 252 $|S_A| = 108, |S_B| = 13, |S_A * S_B| = 1404$

$p = 3, n = 3$ pseudo keys= 11400 good keys= 1032 $|S_A| = 456, |S_B| = 25, |S_A * S_B| = 11400$

4 Future work

Instead of matrices, can we use other mathematical objects?

We don't need commutativity and zero divisors are our friend.

Acknowledgements

We thank Steven Landsburg, R. van Dobben de Bruyn, AAG and SGG and SG for their help.

References

[1] William A. Stein et al. Sage Mathematics Software (Version 9) Project page
Mathoverflow answer

[2] Mathoverflow question Public key cryptography based on non-invertible matrices question

[3] Mathoverflow Public key cryptography based on non-invertible matrices, part II
question