Stickel's Key Agreement Algebraic Variation

Daniel Nager
daniel.nager@gmail.com

May 2024

Abstract

In this document we present a further development of non-commutative algebra based key agreement due to E. Stickel and a way to deal with the algebraic break due to V. Sphilrain.

Introduction

E. Stickel [Sti05] proposed a non-commutative algebra based key agreement further algebraically broken first by V. Sphilrain [Shp08]. Later C. Mullan [Mul11] broke some suggested modifications of Sphilrain in [Shp08].

Here is presented a modification of Stickel's key exchange that circumvents Shpilrain attack. Mullan attack is not relevant here as is a response to Shpilrain proposals to answer his attack, and we address original Sphilrain algebraic break.

Stickel's non-commutative algebra based key agreement

The original Stikel's [Sti05] key exchange is similar in concept to the ordinary Diffie-Hellman key agreement, in particular the operation to get the intermediate value of Alice or Bob the following expressions are used:

$A, B, W \in GL(n, p)$
$AB \neq BA$
$U = A^l W B^m$

From these done both by Alice and Bob a common secret can be agreed, $l, m \in \mathbb{Z}_{p^n}$ is the private key of Alice.

Shpilrain algebraic attack on Stickel's key agreement

The method to break this scheme is to find matrices X,Y such that $XA = AX$, $YB = BY$ and $U = XWY$ and perform algebraic manipulations to get a system of linear equations that allows to recover the shared secret.

In particular X^{-1} is used to get rid of the multivariate equations in $U = XWY$, not solvable by Gaussian elimination, so $U = XWY$ is transformed into $X^{-1}U = WY$, which is now solvable by Gaussian elimination as there's no product of matrices as unknowns.

Proposed variant of Stickel'ls key agreement

The proposed variant is similar but changing the intermediate value, U or V:

$A, B, W \in GL(n, p)$
$AB \neq BA$
$U = A^l W B^m + A^r W B^s$

From these equations a key agreement is done almost the same way, $l, m, r, s \in \mathbb{Z}_{p^n}$ is the private key.

In order to be clear, if V is the intermediate value of Bob, constructed the same way as Alice builds U, to get the shared secret Alice must compute:

$S = A^l V B^m + A^r V B^s$

The question is there's no necessarily a $U = XWY$ for this construction, that will work the same to find the shared secret. We can try to find $U = X_1 W Y_1 + X_2 W Y_2$, but not as a system of linear equations as the inverse of X_1 trick does not work since the second term of the addition remains a product of two unknown matrices, so not solvable as a linear system.

In order to ensure there's no X, Y satisfying $U = XWY$ we need to do, first, ensure U is in $GL(n, p)$, which is not guaranteed. U must be non-singular. Being U non-singular and knowing a matrix is non-singular iff it's the product of non-singular matrices we infer that X and Y must be non-singular as well.

Then, to prove there's no solution to $U = XWY$ we apply the same Shpilrain attack that's not probabilistic or number intensive. We need just to check if the overdetermined system of equations:

$X_1 A = AX_1$
$YB = BY$
$X_1 U = WY$

where X_1 and Y are unknown matrices and the rest known, is inconsistent. If this is the case the exponents used are valid.

Example parameters

As an example parameters for the linear group a minimal non-conservative choice can be $GL(4, p)$ where p is a 16-bit prime. This results in a shared secret of 256-bits and a key size of $4 \cdot p^4 \sim 256$ bits.

References

[Sti05] E. Stickel. "A new public-key cryptosystem in non abelian groups". In: *Proceedings of the Thirteenth International Conference on Information Technology and Applications (ICITA05)* (2005), pp. 426–430.

[Shp08] V. Shpilrain. "Cryptanalysis of Stickel's Key Exchange Scheme". In: *Proceedings of Computer Science in Russia* 5010 (2008), pp. 284–288.

[Mul11] Ciaran Mullan. "Cryptanalysing variants of Stickel's key agreement scheme". In: *Journal of Mathematical Cryptology* 4 (Apr. 2011). DOI: 10.1515/JMC.2011.003.