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:

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

$l, m \in \mathbb{Z}_{p^n}$ is the private key of Alice, and $r, s \in \mathbb{Z}_{p^n}$ is the secret key of Bob. U is the intermediate value send from Alice to Bob, and V the intermediate value send from Bob to Alice, then the shared secret $S \in GL(n, p)$ is:

$S = A^l V B^m = A^r U B^s = A^{l+r} W B^{m+s}$

Shpilrain algebraic attack on Stickel's key agreement

The method to break this scheme is to find matrices $X, Y \in GL(n, p)$ such that:

$XA = AX$
$YB = BY$
$U = XWY$

We need to apply a transformation on the third equation as follows:

$X_1 = X^{-1}$
$X_1 U = WY$

resulting in a overdetermined but consistent system of linear equations:

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

with X and Y found we apply to V value of Bob the following transformation:

$XVY = XA^r WB^s Y = A^r XWYB^s = A^r UB^s = S$

So we get the shared secret without knowledge of the secret keys, just from intermediate values.

Proposed variant of Stickel'ls key agreement

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

$A, B, W \in GL(n, p)$
$AB \neq BA$
$U = A^l WB^m + A^r WB^s$
$V = A^e WB^f + A^g WB^h$

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 of Alice and $e, f, g, h \in \mathbb{Z}_{p^n}$ is the private key of Bob.

U is the intermediate value send from Alice to Bob, and V the intermediate value send from Bob to Alice, then the shared secret $S \in GL(n, p)$ is:

$S = A^l VB^m + A^r VB^s = A^e UB^f + A^g UB^h$
$S = A^{e+l} WB^{f+m} + A^{e+r} WB^{f+s} + A^{g+l} WB^{h+m} + A^{g+r} WB^{h+s}$

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 $U = X_1WY_1 + X_2WY_2$, but not as a system of linear equations as the inverse of X_1 trick does not work as the second term of the addition remains a product of two unknown matrices, so not solvable as a linear system of equations.

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:

$X_1A = AX_1$
$YB = BY$
$X_1U = WY$

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

Simplified version

We can provide a simplified version of the variant that's more elegant and easy to understand, at the price of halving the keyspace of Alice and Bob, the formulas are:

$A, B, W \in GL(n, p)$
$AB \neq BA$
$U = A^lW + WB^s$
$V = A^eW + WB^h$

This is the instance of the scheme when $m = 0$, $r = 0$, $f = 0$ and $g = 0$. As we're presenting in this document just the algebraic circumvention of Shpilrain attack, and not key sizes or parameters n and p in $GL(n, p)$, we can ignore keyspace reduction and take it as a optional scheme.

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.