Contemporary algebraic and geometric techniques in coding theory and cryptography
Summer school — July 18-22, 2022
Università degli Studi della Campania "Luigi Vanvitelli"

SEMIDIRECT PRODUCT KEY EXCHANGE: THE STATE OF PLAY

Christopher Battarbee

Affiliation: University of York
United Kingdom

Abstract

Few fields possess a text as foundational as *New Directions in Cryptography* [1], which presents a key agreement mechanism today known as the Diffie-Hellman Key Exchange (DHKE). The protocol remains relevant in modern cryptographic applications and works by having two parties calculate powers of some agreed-upon group element, say g^a, g^b for g a generator of a cyclic group. Upon receipt of the group element g^b the first party can calculate $(g^b)^a = g^{ab}$; similarly, the second party will also arrive at g^{ab}. If the parties keep their respective exponents a, b secret, they can send the values g^a, g^b in the clear without compromising security - assuming, roughly speaking, that it is computationally expensive to recover an exponent x from knowledge of the generator g and a group element g^x. This problem is known as the discrete logarithm problem (DLP), and can be reduced to a more general problem called the hidden subgroup problem.

Today, the security of DHKE is threatened by Shor's algorithm [2], which is able to efficiently solve the hidden subgroup problem in at least finite abelian groups; i.e., the platform originally proposed for use with DHKE. Since there is a reduction of DLP to a hidden subgroup problem, we consider DHKE to be extremely vulnerable to quantum attack. To this end, the National Security Agency (NSA) announced plans in 2015 to upgrade security standards to so-called 'post-quantum' protocols. In this paper we survey the proposed instances and cryptanalysis of one such protocol.

Armed with the machinery of a more complicated, non-abelian group structure called the semidirect product, we define a key exchange mechanism known as semidirect product key exchange (SDPKE). The proposal in its full generality first appears in [3], although a revised version suggesting a new platform was later published [4].

Since we have fixed our attention of schemes of a particular syntax the main customisable parameter for authors of new proposals is the choice of platform; which in turn, by construction of the semidirect product, depends on a choice of group and automorphism.

In general the literature proceeds somewhat chronologically as new platforms are offered in response to cryptanalysis exploiting some mathematical property of a previously proposed platform. Each proposed platform is some semigroup of matrices; for each proposal we will be required to add, scale and multiply matrices, which in turn means the entries of the matrices must come from a semiring where we have a notion of arithmetic. In particular we do not require division or even subtraction - indeed it has been desirable to specifically preclude the existence of such inverses, essentially because much of the cryptanalytic work has a rather linear algebraic flavour, and many of the results in linear algebra used to attack the schemes are much less powerful in the less structured contexts we consider.

The original proposal in [3] uses matrices over group rings of the form $\mathbb{Z}_p[G]$ where G is non-abelian; this turned out to be vulnerable to a powerful kind of linear algebraic attack developed in [5]; for a special case examination see [6]. The proposal was updated in [4] to matrices over a field occurring as a certain kind of p-group, which makes the attack of [6] much less efficient.

Matrices over the semiring sometimes known as the *tropical* or *min-plus* algebra are considered in [7], partly with the aim of removing some of the linear vulnerability in the above; however, the resulting platform turned out to have a damaging partial order which reduced key recovery, essentially, to binary search [8]. A similar, faster algorithm with a small probability of failure is presented in [9].

The scheme in [7], unlike the original proposal, actually considers matrices under the local notion of addition. Similarly, in [10], one considers the set of matrices over a finite field under addition with an endomorphism defined by multiplication. This mixing of operations seems to defeat the type of attack developed in [5]; however, a new type of attack is introduced in [11] which makes use of an equation known as the *telescoping equality*. The fact that the platform is additive and a full group render [10] particularly vulnerable to this type of attack.

Most recently, in [12], a platform of matrices over a semiring via Boolean algebra has been proposed, with properties that seem to thwart the main types of attack strategy proposed thus far. An attack achieving key recovery has been published [13], but seems to rely on the specific choice of automorphism; that is, does not exploit an inherent weakness of this type of

platform.

The presence of some rarities serving as platforms, many of which are not well-understood, means the scope of further research in the mathematical cryptanalysis of these proposals is quite large. In particular we include in the survey some of the authors' own contributions to the area: in [14] we show that the attack in [11] is actually more powerful than claimed; in [15] that the general telescoping equality-type attack is computationally infeasible to carry out against [12].

Keywords: group-based cryptography, post-quantum cryptography, key exchange protocol

References

[1] Whitfield Diffie and Martin Hellman. "New directions in cryptography". In: *IEEE transactions on Information Theory* 22.6 (1976), pp. 644–654.

[2] Peter W Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th annual symposium on foundations of computer science*. Ieee. 1994, pp. 124–134.

[3] Maggie Habeeb, Delaram Kahrobaei, Charalambos Koupparis, and Vladimir Shpilrain. "Public key exchange using semidirect product of (semi) groups". In: *International Conference on Applied Cryptography and Network Security*. Springer. 2013, pp. 475–486.

[4] Delaram Kahrobaei and Vladimir Shpilrain. "Using semidirect product of (semi) groups in public key cryptography". In: *Conference on Computability in Europe*. Springer. 2016, pp. 132–141.

[5] Alexei Myasnikov and Vitaliĭ Roman'kov. "A linear decomposition attack". In: *Groups Complexity Cryptology* 7.1 (2015), pp. 81–94.

[6] Vitaliĭ Roman'kov. "Linear decomposition attack on public key exchange protocols using semidirect products of (semi) groups". In: *arXiv preprint arXiv:1501.01152* (2015).

[7] Dima Grigoriev and Vladimir Shpilrain. "Tropical cryptography II: extensions by homomorphisms". In: *Communications in Algebra* 47.10 (2019), pp. 4224–4229.

[8] Dylan Rudy and Chris Monico. "Remarks on a tropical key exchange system". In: *Journal of Mathematical Cryptology* 15.1 (2021), pp. 280–283.

[9] Steve Isaac and Delaram Kahrobaei. “A closer look at the tropical cryptography”. In: *International Journal of Computer Mathematics: Computer Systems Theory* (2021), pp. 1–6.

[10] Nael Rahman and Vladimir Shpilrain. “MAKE: A matrix action key exchange”. In: *Journal of Mathematical Cryptology* 16.1 (2022), pp. 64–72.

[11] Daniel Brown, Neal Koblitz, and Jason Legrow. “Cryptanalysis of ‘MAKE’”. In: *eprint.iacr.org.2021.465* (2021).

[12] Nael Rahman and Vladimir Shpilrain. “MOBS: Matrices Over Bit Strings public key exchange”. In: *https://eprint.iacr.org/2021/560* (2021).

[13] Chris Monico. “Remarks on MOBS and cryptosystems using semidirect products”. In: *arXiv preprint arXiv:2109.11426* (2021).

[14] Christopher Battarbee, Delaram Kahrobaei, and Siamak F Shahandashti. “Cryptanalysis of Semidirect Product Key Exchange Using Matrices Over Non-Commutative Rings”. In: *arXiv preprint arXiv:2105.07692* (2021).

[15] Christopher Battarbee, Delaram Kahrobaei, Dylan Tailor, and Siamak F Shahandashti. “On the efficiency of a general attack against the MOBS cryptosystem”. In: *arXiv preprint arXiv:2111.05806* (2021).