

# A LINEAR ATTACK ON A KEY EXCHANGE PROTOCOL USING EXTENSIONS OF MATRIX SEMIGROUPS

JINTAI DING, ALEXEI MIASNIKOV, AND ALEXANDER USHAKOV

**ABSTRACT.** In this paper we analyze the Kahrobaei-Lam-Shpilrain (KLS) key exchange protocols that use extensions by endomorphisms of matrices over a Galois field proposed in [2]. We show that both protocols are vulnerable to a simple linear algebra attack.

**Keywords.** Group-based cryptography, semidirect product, Galois field.

**2010 Mathematics Subject Classification.** 94A60, 68W30.

## 1. INTRODUCTION

The key-exchange protocol proposed by Habeeb, Kahrobaei, Kouparis, and Shpilrain (HKKS) in [1] uses exponentiation in general semidirect products of (semi)groups. When used with an appropriate finite field, it gives the standard Diffie-Hellman protocol based on cyclic groups. The authors of [1] claimed that “when the protocol is used with non-commutative (semi)groups, it acquires several useful features” and proposed a particular platform semigroup which is the extension of the semigroup of  $3 \times 3$  matrices over the group ring  $\mathbb{F}_7[A_5]$  (where  $A_5$  is the alternating group) using inner automorphisms of  $\text{GL}_3(\mathbb{F}_7[A_5])$ . It was shown in [3] that the protocol is susceptible to a simple linear algebra attack.

Later, Kahrobaei, Lam, and Shpilrain in [2] (see also [patent]) proposed two other instantiations of the HKKS protocol that use certain extension of the semigroup of  $2 \times 2$  matrices over the field  $\text{GF}(2^{127})$  and claim that the new protocols are safe for the linear attack described in [3]. In this paper we discuss security properties of the new protocols and show that they are susceptible to attacks similar to those of [3]. A slightly different attack was proposed recently by V. Roman'kov in [4].

## 2. HKKS KEY EXCHANGE PROTOCOL

Let  $G$  and  $H$  be groups, let  $\text{Aut}(G)$  be the group of automorphisms of  $G$ , and let  $\rho : H \rightarrow \text{Aut}(G)$  be a group homomorphism. The *semidirect product* of  $G$  and  $H$  with respect to  $\rho$  is the set of pairs  $\{(g, h) \mid g \in G, h \in H\}$  equipped with the binary operation given by

$$(g, h) \cdot (g', h') = (g^{\rho(h')} g', h \circ h').$$

for  $g \in G$  and  $h \in H$ . It is denoted by  $G \rtimes_{\rho} H$ . Here  $g^{\rho(h')}$  denotes the image of  $g$  under the automorphism  $\rho(h')$ , and  $h \circ h'$  denotes a composition of automorphisms with  $h$  acting first.

Some specific semidirect products can be constructed as follows. First choose your favorite group  $G$ . Then let  $H = \text{Aut}(G)$  and  $\rho = \text{id}_G$ . In which this case the semidirect product  $G \rtimes_{\rho} H$  is called the *holomorph* of  $G$ . More generally, the

---

The work was partially supported by NSF grant DMS-1318716.

group  $H$  can be chosen as a subgroup of  $\mathbf{Aut}(G)$ . Using this construction, the authors of [1] propose the following key exchange protocol.

---

**Algorithm 1.** HKKS key exchange protocol
 

---

**Initial Setup:** Fix the platform group  $G$ , an element  $g \in G$ , and  $\varphi \in \mathbf{Aut}(G)$ . All this information is made public.

**Alice's Private Key:** A randomly chosen  $m \in \mathbb{N}$ .

**Bob's Private Key:** A randomly chosen  $n \in \mathbb{N}$ .

**Alice's Public Key:** Alice computes  $(g, \varphi)^m = (\varphi^{m-1}(g) \dots \varphi^2(g)\varphi(g)g, \varphi^m)$  and publishes the first component  $a = \varphi^{m-1}(g) \dots \varphi^2(g)\varphi(g)g$  of the pair.

**Bob's Public Key:** Bob computes  $(g, \varphi)^n = (\varphi^{n-1}(g) \dots \varphi^2(g)\varphi(g)g, \varphi^n)$  and publishes the first component  $b = \varphi^{n-1}(g) \dots \varphi^2(g)\varphi(g)g$  of the pair.

**Alice's Shared Key:** Alice computes the key  $K_A = \varphi^m(b)a$  taking the first component of the product  $(b, \varphi^n) \cdot (a, \varphi^m) = (\varphi^m(b)a, \varphi^n\varphi^m)$ . (She cannot compute the second component since she does not know  $\varphi^n$ .)

**Bob's Shared Key:** Bob computes the key  $K_B = \varphi^n(a)b$  taking the first component of the product  $(a, \varphi^m) \cdot (b, \varphi^n) = (\varphi^n(a)b, \varphi^m\varphi^n)$ . (He cannot compute the second component since he does not know  $\varphi^m$ .)

---

Note that  $K_A = K_B$  since  $(b, \varphi^n) \cdot (a, \varphi^m) = (a, \varphi^m) \cdot (b, \varphi^n) = (g, \varphi)^n$ . The general protocol described above can be used with any non-abelian group  $G$  and an inner automorphism  $\varphi$  (conjugation by a fixed non-central element of  $G$ ). Furthermore, since all formulas used in the description of this protocol hold if  $G$  is a semigroup and  $\varphi$  is a semigroup automorphism of  $G$ , the protocol can be used with semigroups. The private keys  $m, n$  can be chosen smaller than the order of  $(g, \varphi)$ . For a finite group  $G$ , this can be bounded by  $(\#G) \cdot (\#\mathbf{Aut}(G))$ .

**2.1. Proposed parameters for the HKKS key exchange protocol.** In the original paper [1], the authors propose and extensively analyze the following specific instance of their key exchange protocol. Consider the alternating group  $A_5$ , i.e. the group of even permutations on five symbols (a simple group of order 60) and the field  $\mathbb{F}_7 = \mathbb{GF}(7)$ . Let  $G = \text{Mat}_3(\mathbb{F}_7[A_5])$  be the monoid of all  $3 \times 3$  matrices over the ring  $\mathbb{F}_7[A_5]$  equipped with multiplication. As usual, by  $\mathbf{GL}_3(\mathbb{F}_7[A_5])$  we denote the group of invertible  $3 \times 3$  matrices over the ring  $\mathbb{F}_7[A_5]$ . Fix an inner automorphism of  $G$ , i.e., a map  $\varphi = \varphi_H : G \rightarrow G$  for some  $H \in \mathbf{GL}_3(\mathbb{F}_7[A_5])$  defined by:

$$M \mapsto H^{-1}MH.$$

Clearly, we have  $(\varphi_H)^m = \varphi_{H^m}$  and

$$\begin{aligned} & \varphi_H^{m-1}(M) \dots \varphi_H^2(M)\varphi_H(M)M \\ &= H^{-(m-1)}MH^{m-1} \dots H^{-2}MH^2 \cdot H^{-1}MH^1 \cdot M \\ &= H^{-m}(HM)^m. \end{aligned}$$

This way we obtain the following specific instance of the HKKS key exchange protocol.

---

**Algorithm 2.** HKKS key exchange protocol using  $\text{Mat}_3(\mathbb{F}_7[A_5])$ 


---

**Initial Setup:** Fix matrices  $M \in \text{Mat}_3(\mathbb{F}_7[A_5])$  and  $H \in \mathbf{GL}_3(\mathbb{F}_7[A_5])$ . They are made public.

**Alice's Private Key:** A randomly chosen  $m \in \mathbb{N}$ .

**Bob's Private Key:** A randomly chosen  $n \in \mathbb{N}$ .

**Alice's Public Key:** Alice computes  $A = H^{-m}(HM)^m$  and makes  $A$  public.

**Bob's Public Key:** Bob computes  $B = H^{-n}(HM)^n$  and makes  $B$  public.

**Shared Key:**  $K_A = K_B = H^{-n-m}(HM)^{n+m}$ .

---

The security of this protocol is based on the assumption that, given the matrices  $M \in \text{Mat}_3(\mathbb{F}_7[A_5])$ ,  $H \in \mathbf{GL}_3(\mathbb{F}_7[A_5])$ ,  $A = H^{-m}(HM)^m$ , and  $B = H^{-n}(HM)^n$ , it is hard to compute the matrix  $H^{-n-m}(HM)^{n+m}$ .

In [3] it was shown that the problem above can be easily solved using the fact that  $H$  is invertible. Indeed, any solution of the system:

$$\begin{cases} LA = R, \\ LH = HL, \\ RHM = HMR, \\ L \text{ is invertible,} \end{cases}$$

with unknown matrices  $L, R$  immediately gives the shared key as the product  $L^{-1}BR$ . To solve the system above we describe the set of all solutions to the linear system:

$$\begin{cases} LA = R, \\ LH = HL, \\ RHM = HMR, \end{cases}$$

and try-and-check if  $L$  is invertible for randomly chosen solutions. With high probability a required solution will be found in a few tries.

### 3. DEFENSE AGAINST THE LINEAR ATTACK

The attack described in Section 2.1 splits the public key  $A$  into a product of two “appropriate” matrices  $L, R$  that act as  $H^{-m}$  and  $(HM)^m$ , respectively. The following countermeasure was proposed in [2, Section 5] to prevent the attack. If  $M$  is not invertible, then  $M$  is not invertible and the annihilator of  $HM$ :

$$\text{Ann}(HM) = \{K \in \text{Mat}_3(\mathbb{F}_7[A_3]) \mid K \cdot HM = O\}$$

(where  $O$  is the zero matrix) is not trivial. Since in addition we have  $m, n > 0$ , then adding  $O_A, O_B \in \text{Ann}(HM)$  to the public keys  $A$  and  $B$  changes the keys, but does not change the deduced shared key. This gives the following scheme.

**Algorithm 3.** Modified HKKS key exchange protocol using  $\text{Mat}_3(\mathbb{F}_7[A_5])$

---

**Initial Setup:** Fix matrices  $M \in \text{Mat}_3(\mathbb{F}_7[A_5])$  and  $H \in \mathbf{GL}_3(\mathbb{F}_7[A_5])$ . They are made public.

**Alice's Private Key:** A randomly chosen  $m \in \mathbb{N}$  and  $O_A \in \text{Ann}(HM)$ .

**Bob's Private Key:** A randomly chosen  $n \in \mathbb{N}$  and  $O_B \in \text{Ann}(HM)$ .

**Alice's Public Key:** Alice computes  $A = H^{-m}(HM)^m + O_A$  and makes  $A$  public.

**Bob's Public Key:** Bob computes  $B = H^{-n}(HM)^n + O_B$  and makes  $B$  public.

**Shared Key:**  $K_A = K_B = H^{-n-m}(HM)^{n+m}$ .

---

The idea behind this modification is that one can not simply split  $A$  into a product of two matrices and move one of them to the left hand side. Below, using the property that annihilator is a left ideal and  $H$  is invertible, we show that this is incorrect and the same attack applies. Indeed, it is easy to see that any solution of the system of equations:

$$\begin{cases} LA = R + Z \\ LH = HL \\ R \cdot HM = HM \cdot R \\ Z \cdot HM = O, \\ L \text{ is invertible.} \end{cases}$$

with unknown matrices  $L, R$  and  $Z$ , immediately gives the shared key as the product  $L^{-1}BR$ . It is important that  $H$  is invertible.

#### 4. HKKS PROTOCOL USING AN EXTENSION OF THE SEMIGROUP OF MATRICES OVER A GALOIS FIELD BY AN ENDOMORPHISM

Another countermeasure suggested in [2, Section 4] is to replace the inner automorphism  $\varphi_H$  with a more complex endomorphism. That requires change of the platform semigroup. Consider the semigroup  $G = \text{Mat}_2(\mathbb{G}\mathbb{F}(2^{127}))$  of  $2 \times 2$  matrices over a finite field  $\mathbb{G}\mathbb{F}(2^{127})$ . Let  $\psi$  be the endomorphism of  $G$  which raises every entry of a given matrix to the 4th power:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \xrightarrow{\psi} \begin{bmatrix} a^4 & b^4 \\ c^4 & d^4 \end{bmatrix}.$$

Fix  $H \in \mathbf{GL}_2(\mathbb{G}\mathbb{F}(2^{127}))$  and the corresponding inner automorphism  $\varphi_H$ . Now,  $\varphi = \psi \circ \varphi_H$  with  $\psi$  acting first. This choices give us another instance of the HKKS protocol.

**4.1. Analysis of the protocol.** The map  $x \mapsto x^4$  defined on  $\mathbb{G}\mathbb{F}(2^{127})$  can be recognized as a square of the Frobenius automorphism and, in particular,  $\tau \in \text{Aut}(\mathbb{G}\mathbb{F}(2^{127}))$ . It induces an automorphism  $\psi$  of  $\text{Mat}_2(\mathbb{G}\mathbb{F}(2^{127}))$ :

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \xrightarrow{\psi} \begin{bmatrix} a^4 & b^4 \\ c^4 & d^4 \end{bmatrix}.$$

**Lemma 4.1.**  $|\tau| = 127$  in  $\text{Aut}(\text{Mat}_2(\mathbb{G}\mathbb{F}(2^{127})))$ . Therefore,  $|\psi| = 127$  in  $\text{Aut}(\text{Mat}_3(\mathbb{G}\mathbb{F}(7)))$ .

*Proof.* Consider the Frobenius automorphism  $\rho$  which squares elements of  $\mathbb{G}\mathbb{F}(2^{127})$ . Then  $\rho^{127}(x) = x^{2^{127}} = x$  for every  $x \in \mathbb{G}\mathbb{F}(2^{127})$ . On the other hand, since  $x^{2^k} - x = 0$  can not have more than  $2^k$  solutions in a field, we can deduce that  $|\rho| = 127$ . Now  $|\tau| = |\rho^2| = 127$ .  $\square$

Now,  $\varphi$  is the composition of the endomorphism  $\psi$  and conjugation by  $H$ :

$$\varphi(M) = H^{-1}\psi(M)H$$

for every  $M \in M_2(\mathbb{G}\mathbb{F}(2^{127}))$ . For every  $k \in \mathbb{N}$  we have:

$$\varphi^k(M) = \prod_{i=0}^{k-1} \psi^i(H^{-1}) \cdot \psi^k(M) \cdot \prod_{i=k-1}^0 \psi^i(H).$$

With so defined  $\varphi$ , the Alice's public key  $A = \varphi^{m-1}(M) \dots \varphi(M)M$  is of the form:

$$\begin{aligned} & \left( \prod_{i=0}^{m-1} \psi^i(H^{-1}) \cdot \psi^m(M) \cdot \prod_{i=m-1}^0 \psi^i(H) \right) \cdot \left( \prod_{i=0}^{m-2} \psi^i(H^{-1}) \cdot \psi^{m-1}(M) \cdot \prod_{i=m-2}^0 \psi^i(H) \right) \dots H^{-1}\psi(M)H \cdot M \\ &= \left( \prod_{i=0}^{m-1} \psi^i(H^{-1}) \cdot \psi^m(M) \right) \psi^{m-1}(H) \psi^{m-1}(M) \cdot \psi^{m-2}(H) \psi^{m-2}(M) \dots \psi(H) \psi(M) \cdot H M \\ &= \left( \prod_{i=0}^m \psi^i(H^{-1}) \right) \cdot \left( \prod_{i=m}^0 \psi^i(HM) \right) \end{aligned}$$

Since  $|\psi| = 127$  we can divide  $m = 127 \cdot q + r$  and write the key as follows:

$$A = \left( \prod_{i=0}^{126} \psi^i(H^{-1}) \right)^q \cdot \left( \prod_{i=0}^r \psi^i(H^{-1}) \right) \cdot \left( \prod_{i=r}^0 \psi^i(HM) \right) \cdot \left( \prod_{i=126}^0 \psi^i(HM) \right)^q.$$

The Bob's public key  $B$  is has a similar form (with  $n = 127 \cdot s + t$ ):

$$B = \left( \prod_{i=0}^{126} \psi^i(H^{-1}) \right)^s \cdot \left( \prod_{i=0}^t \psi^i(H^{-1}) \right) \cdot \left( \prod_{i=t}^0 \psi^i(HM) \right) \cdot \left( \prod_{i=126}^0 \psi^i(HM) \right)^s.$$

Now we can use the “old trick”. For each  $0 \leq r \leq 126$  try to solve the system of equations:

$$\begin{cases} L \cdot A = \left( \prod_{i=0}^r \psi^i(H^{-1}) \right) \cdot \left( \prod_{i=r}^0 \psi^i(HM) \right) \cdot R, \\ L \cdot \prod_{i=0}^{126} \psi^i(H^{-1}) = \prod_{i=0}^{126} \psi^i(H^{-1}) \cdot L, \\ R \cdot \prod_{i=126}^0 \psi^i(HM) = \prod_{i=126}^0 \psi^i(HM) \cdot R, \\ L \text{ is invertible.} \end{cases}$$

If the pair  $(L, R)$  satisfies the system above, then  $L^{-1}BR$  is the shared key.

## 5. CONCLUSION

In this paper we analyzed two modifications of the HKKS protocol proposed in [2] and proved that both protocols can be easily broken by simple linear algebra attacks.

## REFERENCES

- [1] M. Habeeb, K. Kahrobaei, C. Kouparis, and V. Shpilrain. Public key exchange using semidirect product of (semi)groups. In *Applied Cryptography and Network Security – ACNS 2013*, volume 7954 of *Lecture Notes Comp. Sc.*, pages 475–486. Springer, 2013.
- [2] D. Kahrobaei, H. Lam, and V. Shpilrain. Public key exchange using extensions by endomorphisms and matrices over a Galois field. Preprint, available at [http://www.sci.ccny.cuny.edu/~shpil/semi\\_galois.pdf](http://www.sci.ccny.cuny.edu/~shpil/semi_galois.pdf).
- [3] A. D. Myasnikov and A. Ushakov. A linear algebra attack to group-ring-based key exchange protocols. In *Applied Cryptography and Network Security – ACNS 2014*, volume 8479 of *Lecture Notes Comp. Sc.*, pages 37–43. Springer, 2014.
- [4] V. Roman'kov. Linear decomposition attack on public key exchange protocols using semidirect products of (semi)groups. preprint. Available at <http://arxiv.org/abs/1501.01152>, 2015.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CINCINNATI, OH, USA  
*E-mail address:* jintai.ding@gmail.com

DEPARTMENT OF MATHEMATICS, STEVENS INSTITUTE OF TECHNOLOGY, HOBOKEN, NJ, USA  
*E-mail address:* amiasnik, aushakov@stevens.edu