A Linear Algebra Attack to Group-Ring-Based Key Exchange Protocols

M. Kreuzer[2], A.D. Myasnikov[1], and A. Ushakov[1,⋆]

[1] Stevens Institute of Technology, Hoboken, NJ, USA
amyasnik,aushakov@stevens.edu
[2] University of Passau, Germany
martin.kreuzer@uni-passau.de

Abstract. In this paper we analyze the Habeeb-Kahrobaei-Koupparis-Shpilrain (HKKS) key exchange protocol which uses semidirect products of groups as a platform. We show that the particular instance of the protocol suggested in their paper can be broken via a simple linear algebra attack.

Keywords: Group-based cryptography, semidirect product, group ring.
Subject Classifications: 94A60, 68W30

1 Introduction

In this paper we study a key-exchange protocol proposed in [1]. The general protocol uses semidirect products of (semi)groups as a platform. One of its special cases is the standard Diffie-Hellman protocol based on cyclic groups. The authors of [1] conjecture that, when the protocol is used with non-commutative (semi)groups, it acquires several useful features. They suggest the extension of a particular non-commutative semigroup of matrices over a certain finite group ring by a conjugation automorphism as a suitable platform. Our main result is that this particular instance of the protocol can be broken using a linear algebra attack.

Before going into details we would like to mention that the semigroup of matrices over a finite group ring has already been used in a cryptographic context, namely in [3] and in [2]. (The former protocol was analyzed in [5].) For a general introduction to non-commutative cryptography we refer to [4].

2 Description of the HKKS Key Exchange Protocol

Let G and H be groups, let $\mathrm{Aut}(G)$ be the group of automorphisms of G, and let $\rho : H \to \mathrm{Aut}(G)$ be a group homomorphism. The *semidirect product* of G

[⋆] The work of the second and third author was partially supported by NSF grant DMS-1318716.

I. Boureanu, P. Owesarski, and S. Vaudenay (Eds.): ACNS 2014, LNCS 8479, pp. 37–43, 2014.

and H with respect to ρ 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 $H = \mathrm{Aut}(G)$ and $\rho = \mathrm{id}_G$. In which this case the semidirect product $G \rtimes_\rho H$ is called the *holomorph* of G. More generally, the group H can be chosen as a subgroup of $\mathrm{Aut}(G)$. 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 $\varphi \in \mathrm{Aut}(G)$. 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 φ^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 φ^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 φ (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 φ 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,ϕ). For a finite group G, this can be bounded by $(\#G)\cdot(\#\,\mathrm{Aut}(G))$. In an actual implementation, the elements a and b would not necessarily be published, but sent to the other party. Hence our security analysis is based on the assumption that an adversary is able to intercept this transmission without being noticed.

3 Proposed Parameters for the HKKS Key Exchange Protocol

In [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. It is a simple group containing 60 elements. We denote its elements by $A_5 = \{\sigma_1, \ldots, \sigma_{60}\}$. Let $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$ be the field with seven elements. Then the group-ring $\mathbb{F}_7[A_5]$ is the set of formal linear combinations

$$A = \sum_{i=1}^{60} a_i \sigma_i,$$

with $a_i \in \mathbb{F}_7$. The addition and multiplication in $\mathbb{F}_7[A_5]$ are defined in the natural way by

$$\left(\sum_{i=1}^{60} a_i\sigma_i\right) + \left(\sum_{i=1}^{60} b_i\sigma_i\right) = \sum_{i=1}^{60}(a_i + b_i)\sigma_i$$

and

$$\left(\sum_{i=1}^{60} a_i\sigma_i\right) \cdot \left(\sum_{i=1}^{60} b_i\sigma_i\right) = \sum_{i=1}^{60} \left(\sum_{\sigma_j\sigma_k=\sigma_i} a_j b_k\right) \sigma_i.$$

By G we denote the monoid of all 3×3 matrices over the ring $\mathbb{F}_7[A_5]$ equipped with multiplication, i.e., we let $G = \mathrm{Mat}_3(\mathbb{F}_7[A_5])$. As usual, by $\mathrm{GL}_3(\mathbb{F}_7[A_5])$ we denote the group of invertible 3×3 matrices over the ring $\mathbb{F}_7[A_5]$.

Furthermore, we choose an inner automorphism of G, i.e., a map $\varphi = \varphi_h : G \to G$ defined by

$$g \mapsto h^{-1}gh,$$

where h is a fixed matrix from $\mathrm{GL}_3(\mathbb{F}_7[A_5])$. Clearly, we have $(\varphi_h)^m = \varphi_{h^m}$ and

$$\varphi^{m-1}(g)\ldots\varphi^2(g)\varphi(g)g = h^{-m+1}gh^{m-1}\ldots h^{-2}gh^2 \cdot h^{-1}gh^1 \cdot g = h^{-m}(hg)^m.$$

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

Algorithm 2. HKKS Key Exchange Protocol Using $\mathrm{Mat}_3(\mathbb{F}_7(A_5))$

Initial Setup: Fix matrices $g \in \mathrm{Mat}_3(\mathbb{F}_7[A_5])$ and $h \in \mathrm{GL}_3(\mathbb{F}_7[A_5])$. 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 $a = h^{-m}(hg)^m$ and makes a public.

Bob's Public Key: Bob computes $b = h^{-n}(hg)^n$ and makes b public.

Shared Key: $K_A = K_B = h^{-n-m}(hg)^{n+m}$.

The security of this protocol is based on the assumption that, given the matrices g, h, $a = h^{-m}(hg)^m$, and $b = h^{-n}(hg)^n$, it is hard to compute the matrix $h^{-n-m}(hg)^{n+m}$. This assumption is similar to the one considered by Stickel in [8] and cryptoanalyzed in [7].

4 Embedding Matrices over Group Rings

In this section we present an embedding of $\mathrm{Mat}_3(\mathbb{F}_7[A_5])$ into $\mathrm{Mat}_{180}(\mathbb{F}_7)$. More generally, fix a finite group $G = \{g_1, \dots, g_k\}$, where $k = \#G$, and a commutative ring R. We want to construct an embedding of $\mathrm{Mat}_n(R[G])$ into $\mathrm{Mat}_{nk}(R)$.

Let $a, b \in R[G]$ and $c = a \cdot b$. We write

$$a = \sum_{g \in G} a_g \cdot g, \;\; b = \sum_{g \in G} b_g \cdot g, \;\;\text{ and }\;\; c = \sum_{g \in G} c_g \cdot g,$$

with $a_g, b_g, c_g \in R$. Next we define a matrix $M_a \in \mathrm{Mat}_k(R)$ and two vectors $\overline{v}_b, \overline{v}_c \in R^k$ as follows:

$$M_a = \begin{pmatrix} a_{g_1 g_1^{-1}} \dots a_{g_1 g_k^{-1}} \\ \dots \\ a_{g_k g_1^{-1}} \dots a_{g_k g_k^{-1}} \end{pmatrix} \text{ and } \overline{v}_b = \begin{pmatrix} b_{g_1} \\ \dots \\ b_{g_k} \end{pmatrix} \text{ and } \overline{v}_a = \begin{pmatrix} c_{g_1} \\ \dots \\ c_{g_k} \end{pmatrix}.$$

Then it is easy to see that

$$M_a \cdot \overline{v}_b = \overline{v}_c. \tag{1}$$

In this way, the left multiplication in $R[G]$ by a corresponds to a linear transformation of R^k and can be naturally represented by a matrix in $\mathrm{Mat}_k(R)$.

Proposition 1. *For $a, b \in R[G]$, we have $M_{a \cdot b} = M_a \cdot M_b$. Furthermore, the map $\Phi : R[G] \to \mathrm{Mat}_k(R)$ given by $a \mapsto M_a$ is a ring monomorphism.*

Proof. Since we obviously have $M_{a+b} = M_a + M_b$, it suffices to prove that $M_{a \cdot b} = M_a \cdot M_b$. For $i, j \in \{1, \dots, n\}$, the entry in position (i, j) of the matrix $M_{a \cdot b}$ is

$$(ab)_{g_i g_j^{-1}} = \sum_{gh = g_i g_j^{-1}} a_g b_h.$$

On the other hand, the entry in position (i, j) of the matrix $M_a \cdot M_b$ is

$$\sum_{m=1}^{k} a_{g_i g_m^{-1}} b_{g_m g_j^{-1}}.$$

Since both elements agree, we have $M_{a \cdot b} = M_a \cdot M_b$. Thus the map $a \mapsto M_a$ is a ring homomorphism. Finally, we note that we can easily reconstruct a from M_a. Consequently, the map $a \mapsto M_a$ is a monomorphism. □

Next, we recall that any matrix $A = (a_{ij}) \in \mathrm{Mat}_n(R[G])$ defines a linear transformation of $(R[G])^n$ in the usual way:

$$\begin{pmatrix} a_{11} \dots a_{1n} \\ \vdots \quad\quad \vdots \\ a_{n1} \dots a_{nn} \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} \sum_i a_{1i} b_i \\ \vdots \\ \sum_i a_{ni} b_i \end{pmatrix}.$$

Our goal is now to extend the above embedding of $R[G]$ to vectors and matrices over $R[G]$. For $A = (a_{ij}) \in \mathrm{Mat}_n(R[G])$, we define a block matrix A^* and for a column vector $\overline{b} = (b_1, \dots, b_n) \in (R[G])^n$, we define a vector $b^* \in R^{kn}$ by

$$A^* = \begin{pmatrix} M_{a_{11}} \dots M_{a_{1n}} \\ \vdots \quad\quad \vdots \\ M_{a_{n1}} \dots M_{a_{nn}} \end{pmatrix} \text{ and } b^* = \begin{pmatrix} \overline{v}_{b_1} \\ \vdots \\ \overline{v}_{b_n} \end{pmatrix}.$$

Let $\overline{c} = A \cdot \overline{b}$. Then it is straightforward to check that we have

$$c^* = A^* \cdot b^*. \tag{2}$$

Proposition 2. *Let G be a finite group of order k and R a commutative ring. Then the map $\varphi : \mathrm{Mat}_n(R[G]) \to \mathrm{Mat}_{nk}(R)$ given by $A \mapsto A^*$ is a ring monomorphism.*

Proof. For $A, B \in M_n(R[G])$, we obviously have $(A+B)^* = A^* + B^*$. It follows from Proposition 1 that

$$A^* \cdot B^* = (AB)^*.$$

Hence the map φ is a ring homomorphism. Finally, we note that φ is injective because, given A^*, one can reconstruct the matrix A from A^*, since every element a_{ij} is repeated on the main diagonal of $M_{a_{ij}}$. □

In particular, there exists an embedding of $\mathrm{Mat}_3(\mathbb{F}_7[A_5])$ into $\mathrm{Mat}_{180}(\mathbb{F}_7)$. The following result characterizes the behavior of invertible matrices under this embedding.

Proposition 3. *For a matrix $A \in \mathrm{Mat}_n(R[G])$ we have*

$$A \in \mathrm{GL}_n(R[G]) \quad \Longleftrightarrow \quad \varphi(A) \in \mathrm{GL}_{nk}(R).$$

Proof. The implication "$\Rightarrow$" follows from the fact that φ is a ring homomorphism. To prove the implication"$\Leftarrow$", we let $\varphi(A) \in \mathrm{GL}_{nk}(R)$. Let $D(x_1, \dots, x_n)$ be the determinant polynomial for matrices of size $n \times n$. Using the rule for determinants of block matrices, we know that $\det(\varphi(A)) = \det(D(M_{a_{11}}, \dots, M_{a_{nn}}))$. The matrix $D(M_{a_{11}}, \dots, M_{a_{nn}})$ is a polynomial expression in the matrices $M_{a_{ij}}$ which represent the left multiplications by the elements a_{ij}. Since the map Φ in Proposition 1 is a ring homomorphism, we see that the matrix $D(M_{a_{11}}, \dots, M_{a_{nn}})$ represents the left multiplication by $D(a_{11}, \dots, a_{nn})$ in $R[G]$. Therefore it is invertible if and only if the element $D(a_{11}, \dots, a_{nn})$ is an invertible element of $R[G]$. This is equivalent to A being an invertible element of $\mathrm{Mat}_n(R[G])$. □

5 A Linear Algebra Attack on the HKKS Key Exchange Protocol

In this section we show that the protocol described in Algorithm 2 can be broken using a linear algebra attack. Thus we are breaking an instance of the computational Diffie-Hellman problem in this specific setting. Our attack provides a full session key recovery and makes only use of the public parameters.

Our first observation is that, to impersonate Alice, we do not need to compute her secret key m. It is sufficient to find two matrices $l, r \in G = \mathrm{Mat}_3(\mathbb{F}_7(A_5))$ satisfying the following system of matrix equations:

$$\begin{cases} l \cdot h = h \cdot l, \\ r \cdot (hg) = (hg) \cdot r, \\ a = lr. \end{cases} \tag{3}$$

Indeed, if we know l and r satisfying the equations above, then we can compute the shared key:

$$\begin{aligned} l \cdot b \cdot r &= l \cdot h^{-n}(hg)^n \cdot r \\ &= h^{-n} lr (hg)^n \\ &= h^{-n} h^{-m} (hg)^m (hg)^n = K. \end{aligned}$$

Our second observation is that system (3) has at least one solution with $l \in \mathrm{GL}_3(\mathbb{F}_7[A_5])$, i.e., with an invertible matrix l, namely $l = h^{-m}$ and $r = (hg)^m$.

Therefore, instead of solving system (3), it suffices to solve the system

$$\begin{cases} \ell \cdot h = h \cdot \ell, \\ r \cdot (hg) = (hg) \cdot r, \\ \ell a = r \end{cases} \tag{4}$$

and to recover the matrix l from the equation $\ell \cdot l = 1$.

Our final observation is that, using the embedding of Section 4, the system (4) can be transformed to a system of linear equations over $\mathbb{F}_7$. Indeed, we can write the matrix ℓ in the form

$$\ell = \begin{pmatrix} \sum_{i=1}^{60} l_i^{(1,1)} \sigma_i & \sum_{i=1}^{60} l_i^{(1,2)} \sigma_i & \sum_{i=1}^{60} l_i^{(1,3)} \sigma_i \\ \sum_{i=1}^{60} l_i^{(2,1)} \sigma_i & \sum_{i=1}^{60} l_i^{(2,2)} \sigma_i & \sum_{i=1}^{60} l_i^{(2,3)} \sigma_i \\ \sum_{i=1}^{60} l_i^{(3,1)} \sigma_i & \sum_{i=1}^{60} l_i^{(3,2)} \sigma_i & \sum_{i=1}^{60} l_i^{(3,3)} \sigma_i \end{pmatrix}$$

with unknown coefficients $l_i^{(j,k)} \in \mathbb{F}_7$. Similarly, we can write the matrix r with unknown coefficients $r_i^{(j,k)} \in \mathbb{F}_7$. After performing all matrix multiplications in (4) and applying the embedding of Section 4, we obtain a system of 1620 linear equations in 1080 unknowns $l_i^{(j,k)}, r_i^{(j,k)}$ over the field $\mathbb{F}_7$.

Thus, to break the key exchange protocol, we can proceed as follows.

(1) First we find *any* solution of the described linear system arising from (4) that defines a non-singular matrix ℓ. We know that such a solution exists, since

$\ell = h^{-1}$ and $r = hg$ solve the system. Let us check that randomly chosen solutions of the linear system will lead to a non-singular matrix ℓ with high probability.

In Section 4 we showed that there exists an embedding φ of $M_3(\mathbb{F}_7[A_5])$ into $M_{180}(\mathbb{F}_7)$. By Proposition 3, the matrix ℓ is invertible if and only if $\varphi(\ell)$ is invertible, and this is equivalent to $\det(\varphi(\ell)) \neq 0$. The determinant $\det(\varphi(\ell))$ is a polynomial in the unknowns $l_i^{(j,k)}, r_i^{(j,k)}$ with coefficients from the field $\mathbb{F}_7$. By the Schwartz–Zippel Lemma (see [9,6]), the probability to randomly select a singular solution is at most $1/7$. Hence a sequence of, say 100, trials will produce a non-singular solution of System (4) with very high probability.

(2) After having found ℓ, the determination of l requires merely the solution of another (smaller) linear system corresponding to $l \cdot \ell = I$. Since ℓ is invertible, there is a unique solution for l.

(3) Finally, the computation of the product $l \cdot b \cdot r = K$ reveals the private key.

References

1. Habeeb, M., Kahrobaei, D., Koupparis, C., Shpilrain, V.: Public key exchange using semidirect product of (semi)groups. In: Jacobson, M., Locasto, M., Mohassel, P., Safavi-Naini, R. (eds.) ACNS 2013. LNCS, vol. 7954, pp. 475–486. Springer, Heidelberg (2013)
2. Kahrobaei, D., Koupparis, C., Shpilrain, V.: A CCA secure cryptosystem using matrices over group rings, `http://www.sci.ccny.cuny.edu/~shpil/res.html` (preprint)
3. Kahrobaei, D., Koupparis, C., Shpilrain, V.: Public key exchange using matrices over group rings. Groups, Complexity, Cryptology 5, 97–115 (2013)
4. Miasnikov, A.G., Shpilrain, V., Ushakov, A.: Non-Commutative Cryptography and Complexity of Group-Theoretic Problems. Mathematical Surveys and Monographs. AMS (2011)
5. Myasnikov, A.D., Ushakov, A.: Quantum algorithm for discrete logarithm problem for matrices over finite group rings, `http://eprint.iacr.org/2012/574` (preprint)
6. Schwartz, J.: Fast probabilistic algorithms for verification of polynomial identities. JACM 27, 701–717 (1980)
7. Shpilrain, V.: Cryptanalysis of Stickel's key exchange scheme. In: Hirsch, E.A., Razborov, A.A., Semenov, A., Slissenko, A. (eds.) CSR 2008. LNCS, vol. 5010, pp. 283–288. Springer, Heidelberg (2008)
8. Stickel, E.: A new method for exchanging secret keys. In: Proceedings of the Third International Conference on Information Technology and Applications (ICITA 2005). Contemporary Mathematics, vol. 2, pp. 426–430. IEEE Computer Society (2005)
9. Zippel, R.: Probabilistic algorithms for sparse polynomials. In: Ng, E.W. (ed.) Symbolic and Algebraic Computation. LNCS, vol. 72, pp. 216–226. Springer, Heidelberg (1979)