Cryptanalysis of a key agreement scheme using determinants and rectangular matrices

Daniel R. L. Brown

January 26, 2023

Abstract

Hecht and Scolnik proposed key agreement using rectangular matrices and determinants. This report describes an attack.

1 Introduction

Hecht and Scolnik, in IACR eprint 2022/1370 on 2022 Oct 12, proposed key agreement where the private keys are pairs of rectangular matrices, the public keys are square matrices, and the shared secrets are computed using a determinant of the products of the private key matrices and the peer's public key matrix.

This report describes an attack on a crucial step of the proposed key agreement. This attack was communicated privately to Hecht and Scolnik, who then removed this particular proposal from their IACR eprint 2022/1370, and kindly acknowledged me.

1.1 Related previous work

To be completed.

2 Summary of the proposed key agreement

This section paraphrases the main part of the proposed key agreement.

1. Alice's private key $a = (a_1, a_2)$ consists of a pair of two rectangular $r \times c$ matrices, where $r > c$. The matrix entries of a_1 and a_2 should be selected uniformly at random from a fixed finite field, such as the ring of integers modulo a 32-bit prime.

2. Alice's public key is the square $r \times r$ matrix:

$$A = a_1 a_2^t, \tag{1}$$

   where a_2^t is the matrix transpose of a_2, and all arithmetic is done with the chosen finite field.

3. Bob does the same steps as Alice, with private key (b_1, b_2) and public key $B = b_1 b_2^t$.

4. Alice receives Bob's public key B, she computes a shared secret key:

$$k_{a,B} = \det(a_1^t B a_2), \tag{2}$$

   using her private key a and Bob's public key B.

5. Bob similarly computes a shared secret key $k_{b,A} = \det(b_1^t A b_2)$.

Hecht and Scolnik proved that the two shared secret keys are equal, and the proof is repeated here for convenience:

Lemma 1. *Alice's and Bob's shared secret keys are equal:*

$$k_{a,B} = k_{b,A}. \tag{3}$$

Proof. Calculate as follows:

$$\begin{aligned} k_{a,B} &= \det(a_1^t B a_2) \\ &= \det(a_1^t b_1 b_2^t a_2) \\ &= \det((a_1^t b_1)(b_2^t a_2)) \\ &= \det(a_1^t b_1) \det(b_2^t a_2) \\ &= \det((a_1^t b_1)^t) \det((b_2^t a_2)^t) \\ &= \det(b_1^t a_1) \det(a_2^t b_2) \\ &= \det(b_1^t a_1 a_2^t b_2) \\ &= \det(b_1^t A b_2) \\ &= k_{b,A}. \end{aligned} \tag{4}$$

□

3 An attack

We show how to compute shared secret key $k_{a,B}$ from the two public keys A and B. The attack involves computing the characteristic polynomial of A^tB.

Lemma 2. *Let x be an indeterminate variable. Then*

$$\det(xI_r - A^tB) = x^r + \cdots + (-1)^c k_{a,B} x^{r-c}. \tag{5}$$

In particular, the shared secret $k_{a,B}$ can be obtained by multiplying the coefficient of x^{r-c} in the characteristic polynomial of the publicly computable square matrix A^tB by $(-1)^c$.

Proof. Let a'_1 be the square $r \times r$ matrix obtained from a_1 by padding it with $r - c$ columns of all zeros on the right. Define matrices a'_2 and b'_1 and b'_2 similarly. Notice that:

$$A = a'_1(a'_2)^t, \tag{6}$$

so, the padded private key can be considered equivalent to the original private key, at least for the purpose of the computation of the public key.

However, for the computing the secret key, the padded columns create extra columns rows, making a block decomposition like this:

$$M = (a'_1)^t B a'_2 = \begin{pmatrix} a_1^t B a_2 & 0 \\ 0 & 0 \end{pmatrix}. \tag{7}$$

Alice's shared secret is obtained by computing the determined of the upper left block of M. The matrix M is not public.

The determinant of M is 0, because, for example, of the lower right block of all zeros. But it has a nonzero characteristic polynomial that contains the Alice's shared secret, because of the following calculation:

$$\begin{aligned} p_M(x) &= \det(xI_r - M) \\ &= \det(xI_r - (a'_1)^t B a'_2) \\ &= \det \begin{pmatrix} xI_c - a_1^t B a_2 & 0 \\ 0 & xI_{r-c} \end{pmatrix} \\ &= \det(xI_c - a_1^t B a_2) \det(xI_{r-c}) \\ &= (x^c + \cdots + (-1)^c \det(a_1^t B a_2))(x^{r-c}) \\ &= x^r + \cdots + (-1)^c k_{a,B} x^{r-c}. \end{aligned} \tag{8}$$

The matrix M is not public. However, we next show that M has the same characteristic polynomial as a publicly computable matrix.

Characteristic polynomials of matrices obey the following interesting commutation rule $p_{UV}(x) = p_{VU}(x)$. Using this commutation rule in the following calculation

$$\begin{aligned} p_M(x) &= p_{((a_1')^t B) a_2'}(x) \\ &= p_{a_2'((a_1')^t B)}(x) \\ &= p_{((a_2')(a_1')^t) B}(x) \\ &= p_{A^t B}(x). \end{aligned} \tag{9}$$

So, now we can compute the characteristic polynomial of M, using that of $A^t B$, in this way extract the shared secret key $k_{a,B}$. □

4 A small example

In this example, we use integers modulo the prime $p = 283$ as the finite field to which all matrix entries belong.

4.1 A key agreement session

Let Alice's private key be:

$$(a_1, a_2) = \left(\begin{pmatrix} 226 & 197 \\ 107 & 43 \\ 21 & 192 \\ 144 & 172 \end{pmatrix}, \begin{pmatrix} 184 & 101 \\ 21 & 247 \\ 249 & 227 \\ 120 & 1 \end{pmatrix} \right), \tag{10}$$

which was chosen somewhat randomly. Then, Alice's public key is:

$$A = a_1 a_2^t = \begin{pmatrix} 70 & 201 & 245 & 149 \\ 259 & 133 & 180 & 148 \\ 50 & 38 & 137 & 165 \\ 3 & 228 & 188 & 189 \end{pmatrix}. \tag{11}$$

For example, the lower right entry of matrix A can be computed, by standard matrix definitions, by taking the dot product of the last row of a_1 with last row of a_2:

$$\begin{aligned}\begin{pmatrix}144 & 172\end{pmatrix}\begin{pmatrix}120\\1\end{pmatrix} &= 144 \times 120 + 172 \times 1\\ &= 17280 + 172\\ &= (283 \times 61 + 17) + 172 = (283 \times 61) + 189\\ &\equiv 189 \bmod 283.\end{aligned}$$

Similarly, let Bob's private key and public key be:

$$(b_1, b_2) = \left(\begin{pmatrix}139 & 83\\223 & 84\\159 & 25\\115 & 29\end{pmatrix}, \begin{pmatrix}144 & 148\\59 & 266\\124 & 267\\65 & 265\end{pmatrix}\right), \tag{12}$$

$$B = b_1 b_2^t = \begin{pmatrix}38 & 281 & 60 & 183\\113 & 126 & 272 & 248\\277 & 183 & 72 & 263\\193 & 66 & 212 & 161\end{pmatrix}. \tag{13}$$

Alice computes her copy of the shared secret key by the computation:

$$\begin{aligned}k_{a,B} &= \det(a_1^t B a_2)\\ &= \det\begin{pmatrix}173 & 119\\178 & 78\end{pmatrix}\\ &= -7688\\ &= (283 \times (-27)) + 236\\ &= 236.\end{aligned} \tag{14}$$

4.2 Attacking the session

The characteristic polynomial of matrix $A^t B$ is:

$$\det(xI_4 - A^t B) = x^4 + 32x^3 + 236x^2, \tag{15}$$

with all computations done modulo $p = 283$.

The coefficient of $x^{r-c} = x^{4-2} = x^2$ is 236. Multiplying this by $(-1)^c = (-1)^2 = 1$ gives 236, which is $k_{a,B}$.

5 Cost analysis

Several well-known methods are available to compute a characteristic polynomial. The example above was computed using a variant of Lagrange interpolation. First, the determinant was evaluated at some specific values of x. Each such specific determinant provides a linear equation on the unknowns, namely the coefficients of the characteristic polynomial. With sufficiently many equations, this system of equations can be solved.

An alternative approach would be to use the Cayley-Hamilton theorem. This approach uses the fact that $p(A^tB) = 0$ where $p(x)$ is the characteristic polynomial of A^tB. Computing the powers $(A^tB)^j$ for $0 \leq j \leq r$, renders the single matrix equation $p(A^tB) = 0$ into a system of linear equations about our unknowns, namely the coefficient of the characteristic polynomial $p(x)$.

There are only really c unknown coefficients in the characteristic polynomial. Cramer's rule shows that, solving of one of the unknowns, for us, the coefficient of x^{r-c}, generally costs roughly two computation of $c \times c$ determinants, and a division in the field. (The exception to this generality is that, sometimes, Cramer's would involve division by zero.)

So, with this approach, the attacker's computational cost is approximately:

1. the combined computational cost of Alice and Bob,

2. a field division, and

3. r multiplications of $r \times r$ matrices,

Usually, the majority of the attack cost would be this third part, which is to compute the matrix A^tB and its r powers. This latter part costs at most $2r^4$ field operations.