CRYPTANALYSIS OF THE MORE SYMMETRIC KEY FULLY HOMOMORPHIC ENCRYPTION SCHEME

BOAZ TSABAN AND NOAM LIFSHITZ

ABSTRACT. The fully homomorphic symmetric encryption scheme *MORE* encrypts keys by conjugation with a random invertible matrix over an RSA modulus. We provide a two known-ciphertexts cryptanalysis recovering a linear dependence among the two encrypted keys.

1. THE FHE SCHEME MORE

In their paper [1], Kipnis and Hibshoosh propose, among other things, to use the following type of fully homomorphic encryption (FHE) of keys, which they named *Matrix Operation for Randomization or Encryption (MORE).*

Let N be an RSA modulus. The secret key is an invertible matrix $A \in \mathrm{GL}_2(\mathbb{Z}_N)$. The scheme only encrypts random elements $k \in \mathbb{Z}_N$, and is constrained not to encrypt the same element twice. The encryption is randomized. To encrypt a key k, choose a random secret $s \in \mathbb{Z}_N$, and output

$$E_A(k) := A^{-1} \begin{pmatrix} s & 0 \\ 0 & k \end{pmatrix} A.$$

To decrypt, conjugate by A^{-1} instead of A. It is immediate that this is a fully homomorphic function of k.

This scheme is proved to be secure in the sense that, given encryptions of uniformly random, independent keys $k_1, \dots, k_n$, for arbitrary n, one can learn nothing about the key k_1 [1, page 12].

A second FHE proposed in [1], *Polynomial Operation for Randomization or Encryption (PORE)*, is shown there to be equivalent to MORE.

An application to signatures is provided in [1], but Hibshoosh reported to us that this specific application has in the meanwhile been cryptanalyzed.

2. CRYPTANALYSIS OF MORE

We do not invalidate the Kipnis-Hibshoosh proof of security. But we identify another potential problem with improper uses of this scheme.

Lemma 2.1. *A 2×2 matrix commutes with all diagonal matrices if an only if it is diagonal.*

Proof. It is necessary that C commutes with the basis matrix E_{11}, which implies that the off-diagonal entries of C are 0. Thus, C is diagonal. Being diagonal is also sufficient for C commuting with all diagonal matrices. □

Lemma 2.2. *Each matrix A with nonzero diagonal entries is of the form*

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & * \\ * & 1 \end{pmatrix}.$$

Proof. We have that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & b/a \\ c/d & 1 \end{pmatrix}.$$ □

The cryptanalysis. Let A be the secret matrix. We may assume that the diagonal entries of A are nonzero,[1] and thus write

$$A = D \begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix},$$

where D is diagonal invertible. As diagonal matrices commute, we have that

$$\begin{aligned} E_A(k) &= A^{-1} \begin{pmatrix} s & 0 \\ 0 & k \end{pmatrix} A = \begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix}^{-1} D^{-1} \begin{pmatrix} s & 0 \\ 0 & k \end{pmatrix} D \begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix}^{-1} \begin{pmatrix} s & 0 \\ 0 & k \end{pmatrix} \begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix}. \end{aligned}$$

Let $E_A(k) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is given, we obtain the equation

$$\begin{aligned} \begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} &= \begin{pmatrix} s & 0 \\ 0 & k \end{pmatrix} \begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix}; \\ \begin{pmatrix} \alpha + b\gamma & \beta + b\delta \\ c\alpha + \gamma & c\beta + \delta \end{pmatrix} &= \begin{pmatrix} s & sb \\ kc & k \end{pmatrix}. \end{aligned}$$

In particular, we have that

$$k = \beta c + \delta,$$

[1] This will be the case, with overwhelming probability. One can address specifically degenerated cases, but there is no need for that: We may randomize A. Indeed, choose a uniformly random invertible matrix B. Then so is AB, regardless of the way A was chosen, and we have that $E_{AB}(k) = B^{-1}E_A(k)B$, which can be computed from the encrypted matrix and B.

where only c is unknown. Recall that c depends only on A.

Now, assume that keys k_1, k_2 are encrypted. Then, in terms of the matrices forming the encryptions, we have that

$$\begin{aligned} k_1 &= \beta_1 c + \delta_1; \\ k_2 &= \beta_2 c + \delta_2. \end{aligned}$$

This can be recast as a known, nontrivial linear equation satisfied by k_1, k_2.

3. Discussion

3.1. **Destructive comments.** Consider a scenario that keys are distributed to many independent users. Having any of the keys compromised, we can find all other keys by the known linear equations. Another view is that the entropy of any set of encrypted key is reduced, given the ciphertexts, to that of a single key. It follows that one can encrypt once safely, but probably not more with MORE.

This attack works even if we only have the second column of the encrypted matrix. We obtain similar equations for s (the randomization) and the other entries of the (simplified) secret matrix. All entropy reduces to that of one entry.

Our attack generalizes to the general case of $n \times n$ matrices as follows: Consider MORE, where given a key k one choses $n-1$ random elements $s_1, \ldots, s_{n-1}$, and the encryption is

$$E_A(k) := A^{-1} \operatorname{diag}(s_1, \ldots, s_{n-1}, k) A.$$

Given n encryptions of keys $k_1, \ldots, k_n$, one can express k_n as a linear combination of $k_1, \ldots, k_{n-1}$. Even worse, the same holds if the encryption is

$$E_A(k) := A^{-1} \left(S \oplus (k) \right) A$$

for S a random secret $n-1 \times n-1$ matrix. It seems that there is no way to add to MORE more randomization than that, if we wish to maintain its homomorphic (in k) properties.

If we are fine with deterministinc encryption, then we may consider the encryption of secret $n \times n$ key *matrices* K by

$$E_A(K) := A^{-1} K A.$$

This is fully homomorphic (with respect to addition and multiplication of matrices), though not randomized. But then we also have a problem: Given $n^2 + 1$ encrypted keys, one can express any of them as a linear combination of the others, since the matrices

$$E_A(K_1), \ldots, E_A(K_{n^2+1})$$

are linearly dependent and conjugation is an automorphism.

3.2. **Constructive comments.** In reply to our observation, Kipnis and Hibshoosh (personal communication) point out the following potential use of MORE: For each new key k, we generate a *new* random matrix A and encrypt k. Then, we can send the output to a computationally stronger server, that will evaluate a (univariate) polynomial $f(x)$ of our choice on $E_A(k)$ and send us back, so we can decrypt and find $f(k)$. In light of our observation, the server may, instead, find a linear relation $f(k) = \alpha k + \beta$ and send the pair (α, β) instead, in the clear. This will save communication and time for the weaker server, and is equally secure.

The Kipnis–Hibshoosh idea is also interesting in the general setting: Assume that the conjugacy problem over a certain ring R is difficult. Then conjugation by a secret matrix is a symmetric (nonrandomized–but there may be solutions to that) FHE scheme, with respect to the ring addition and multiplication. Are there suitable rings for that purpose?

Acknowledgments. We thank Aviad Kipnis and Eliphas Hibshoosh for their feedback on this note.

References

[1] A. Kipnis and E. Hibshoosh, *Efficient Methods for Practical Fully Homomorphic Symmetric-key Encrypton, Randomization and Verification*, Cryptology ePrint Archive, Report 2012/637.

(Tsaban) Department of Mathematics, Bar-Ilan University, Ramat Gan 5290002, Israel and Department of Mathematics, Weizmann Institute of Science, Rehovot 7610001, Israel
E-mail address: tsaban@math.biu.ac.il
URL: www.cs.biu.ac.il/~tsaban

(Lipshitz) Department of Mathematics, Bar-Ilan University, Ramat Gan 5290002, Israel
E-mail address: noamlifshitz@gmail.com