SCIS 2012 The 29th Symposium on
Cryptography and Information Security
Kanazawa, Japan, Jan. 30 - Feb. 2, 2012
The Institute of Electronics,
Information and Communication Engineers

An attack against a key-agreement protocol proposed by Accardi et al.

Keita Xagawa *

Abstract— In July 2011, Accardi, Iriyama, Regoli, and Ohya proposed a key-agreement framework over a semigroup. Their framework can be considered as a generalization of the Diffie-Hellman key-agreement protocol. They proposed a variant of the Diffie-Hellman key-agreement protocol and a matrix-based key-agreement protocol.

In this paper, we propose a passive attack against the matrix-based key-agreement protocol. We describe how an eavesdropper computes a session key between legitimate users.

Keywords: key-agreement protocols, cryptanalysis, a ring of matrices, vectorization, the Kronecker product.

1 Introduction

In July 2011, Accardi, Iriyama, Regoli, and Ohya proposed a key-agreement framework over a semigroup [AIRO11b], which captures the Diffie-Hellman key-agreement protocol. They also instantiated concrete key-agreement protocols using their framework.

One of them [AIRO11a] is based on the ring of matrices over a finite field, $M(\mathbb{F}, d)$. Ref. [AIRO11a] reported implementation results but gave no security proof. It is hard to say that they assessed its security sufficiently even for an eavesdropper.

This paper proposes a practical attack against the protocol [AIRO11a] that an eavesdropper can computes a session key between legitimate users.

Notes: Accardi et al. have already noticed the attack [July 2011, private communication]. (As a pointer, we refer to Accardi's slides [Acc11].) They already proposed an alternative protocol [Acc11]. However, Accardi found an attack against their alternative protocol [July 2011, private communication]. We also give an attack against the alternative protocol, which is essentially the same as Accardi's.

For clearness, we call the protocol in [AIRO11a] and the alternative, the AIRO-T1 protocol and the AIRO-T2 protocol, respectively.

Related Works: There are several proposals of key-agreement protocol employing semigroups and attacks against them. See, e.g., Blackburn and Galbraith [BG99, Sect. 1], and [Zum08, Sect. 2.4] for summary.

Notation: We change notation from the original paper to reduce subscripts. Let $\mathbb{S}$ denote a multiplicative semigroup. For $\alpha \in \mathbb{S}$, $\mathbb{S}_\alpha$ denotes a semigroup defined by α, i.e., $\mathbb{S}_\alpha = \{\alpha^n : n \in \mathbb{N}\}$. $\mathrm{Mor}(\mathbb{S}_\alpha, \mathbb{S})$ denotes the set of homomorphisms from $\mathbb{S}_\alpha$ to $\mathbb{S}$.

* NTT Information Sharing Platform Laboratories, 3-9-11 Midori-cho, Musashino-shi, Tokyo, 180-8585 Japan, xagawa.ketia@lab.ntt.co.jp

We consider a finite field, denoted by $\mathbb{F}$, of order q. For field $\mathbb{F}$ and natural integer d, $M(\mathbb{F}, d)$ denotes the ring of d by d matrices over $\mathbb{F}$. $\mathrm{GL}(\mathbb{F}, d)$ denotes general linear group induced from $M(\mathbb{F}, d)$. We denote a zero matrix and an identity matrix in $M(\mathbb{F}, d)$ by O and I, respectively. For natural number d, $[d]$ denotes $\{0, 1, \ldots, d-1\}$. For matrix S, $S^\top$ denotes the transpose of S.

Vectorization and the Kronecker product: We will employ the relations between the Kronecker product and vectorization. These relations are found in the textbooks on matrices, and Magnus and Neudecker [MN79].

Define vectorization function $\mathrm{vec} : M(\mathbb{F}, d) \to \mathbb{F}^{d^2}$ by

$$\mathrm{vec}(X) = (X_{0,0}, X_{0,1}, \ldots, X_{0,d-1}, \ldots, X_{d-1,0}, \ldots, X_{d-1,d-1}),$$

that is, the concatenations of the row vectors of X. Let $\otimes$ denote the Kronecker product. For two matrices $S, T \in M(\mathbb{F}, d)$, the Kronecker product of S and T is defined as the matrix

$$S \otimes T = \begin{bmatrix} s_{0,0}T & \cdots & s_{0,d-1}T \\ \vdots & \ddots & \vdots \\ s_{d-1,0}T & \cdots & s_{d-1,d-1}T \end{bmatrix} \in M(\mathbb{F}, d^2).$$

For any $S, T, X \in M(\mathbb{F}, d)$, we have that

$$\mathrm{vec}(S \cdot X \cdot T) = \mathrm{vec}(X) \cdot (S^\top \otimes T).$$

From the property of the Kronecker product, if $S, T \in \mathrm{GL}(\mathbb{F}, d)$ then $S^\top \otimes T \in \mathrm{GL}(\mathbb{F}, d^2)$.

2 Review of the Framework

Let c and d be efficiently computable and invertible functions from $\mathbb{S}$ to $\mathbb{S}$. Let $e, f, g, h : \mathbb{S} \to \mathbb{S}$ be arbitrary functions.

Suppose that the following conditions hold:

- $e \circ f = g \circ h$ holds over $\mathbb{S}_\alpha$.
- $c \circ f \in \mathrm{Mor}(\mathbb{S}_\alpha, \mathbb{S})$.

Accardi et al. proposed the following framework of key agreement between an initiator and a responder, denoted by $\mathcal{I}$ and $\mathcal{R}$.

- $\mathcal{I}, \mathcal{R}$: Both parties share the parameters, $\mathbb{S}$ and α.
- $\mathcal{I} \to \mathcal{R}$: Choose c, d, e, f, g, h. Send $e \circ c^{-1}$, $d^{-1} \circ h$, $\beta = c \circ f(\alpha)$.
- $\mathcal{R} \to \mathcal{I}$: Choose $x \leftarrow \mathbb{N}$. Send $\gamma = d^{-1} \circ h(\alpha^x)$.
- $\mathcal{I}$: Compute $\kappa = g \circ d(\gamma)$ $(= g \circ h(\alpha^x))$.
- $\mathcal{R}$: Compute $\kappa = e \circ c^{-1}((c \circ f(\alpha))^x)$ $(= e \circ c^{-1}(c \circ f(\alpha^x)) = e \circ f(\alpha^x))$.

3 The AIRO-T1 Protocol and Our Attack

We review the AIRO-T1 protocol [AIRO11a] and give our attack.

3.1 The AIRO-T1 Protocol

Set $\mathbb{S} = M(\mathbb{F}, d)$. Let G be an element in $M(\mathbb{F}, d)$, whose orbit is exponentially long in d, as α.

Accardi et al. set $\pi_0(X) = \sum_{i=0}^{M} A_i X^i B_i$, $\pi_1(X) = aX + bI$, and $\pi_2(X) = PX^nP^{-1}$, where $A_i, B_i \in M(\mathbb{F}, d)$, $a, b \in \mathbb{F}$, and $P \in \mathrm{GL}(\mathbb{F}, d)$. Let $\rho(X) = AXB^{-1} + C$, where $A, B \in \mathrm{GL}(\mathbb{F}, d)$ and $C \in M(\mathbb{F}, d)$.

They instantiated their key-exchange protocol by setting

- $\mathbb{S} = M(\mathbb{F}, d)$, $\alpha = G$,
- $c = id$, $d = \rho^{-1}$,
- $e = \pi_0 \circ \pi_1$, $f = \pi_2$, $g = \pi_0$, and $h = \pi_1 \circ \pi_2$.

Obviously, we have that $\pi_0 \circ \pi_1 \circ \pi_2 = e \circ f = g \circ h$. The shared key is $K = \pi_0 \circ \pi_1 \circ \pi_2(G^x)$.

Their protocol is summarized as follows:

- $\mathcal{I}, \mathcal{R}$: Both parties share the parameters, $\mathbb{F}$, d, and G.
- $\mathcal{I} \to \mathcal{R}$: Choose $\pi_0, \pi_1, \pi_2, \rho$ by generating $A_i, B_i, C \in M(\mathbb{F}, d)$, $a, b, \in \mathbb{F}$, $A, B, P \in \mathrm{GL}(\mathbb{F}, d)$ and $n \in \mathbb{N}$ randomly. Send $\pi_0 \circ \pi_1$, $\rho \circ \pi_1$ (rather than $\rho \circ \pi_1 \circ \pi_2$), and $M = \pi_2(G)$.
- $\mathcal{R} \to \mathcal{I}$: Choose $x \leftarrow \mathbb{N}$. Send $R = \rho \circ \pi_1(M^x)$ $(= \rho \circ \pi_1 \circ \pi_2(G^x))$.
- I: Compute $K = \pi_0 \circ \rho^{-1}(R)$ $(= \pi_0 \circ \pi_1 \circ \pi_2(G^x))$.
- R: Compute $K = \pi_0 \circ \pi_1(M^x)$ $(= \pi_0 \circ \pi_1 \circ \pi_2(G^x))$.

We note that, in their scheme, $\mathcal{I}$ sends $(F, AbB^{-1} + C)$ as $\rho \circ \pi_1$, where

$$F = \{f_{i,j,j_1,j_2}\}_{i,j,j_1,j_2 \in [d]} = \{(Aa)_{i,j_1}(B^{-1})_{j_2,j})\}_{i,j,j_1,j_2 \in [d]}.$$

By using F, $\mathcal{R}$ can compute $X \mapsto Y = Aa \cdot X \cdot B^{-1}$ by, for $i, j \in [d]$,

$$Y_{i,j} = \sum_{j_1,j_2 \in [d]} (Aa)_{i,j_1}(X)_{j_1,j_2}(B^{-1})_{j_2,j} = \sum_{j_1,j_2 \in [d]} f_{i,j,j_1,j_2}(X)_{j_1,j_2}.$$

The responder, $\mathcal{R}$, computes $R = \rho \circ \pi_1(M^x) = AaM^xB^{-1} + AbB^{-1} + C$ using F and $AbB^{-1} + C$.

3.2 Our Attack

Apparently, the eavesdropper obtains $\pi_0 \circ \pi_1$, $\rho \circ \pi_1$, and $R = \rho \circ \pi_1(M^x)$. If one can retrieve M^x from $\rho \circ \pi_1$ and R, then one can compute $K = \pi_0 \circ \pi_1(M^x)$ as $\mathcal{R}$ does.

The eavesdropper has

$$\rho \circ \pi_1 = (F, AbB^{-1} + C),$$
$$R = Aa \cdot M^x \cdot B^{-1} + AbB^{-1} + C.$$

The problem is reduced to finding M^x from

$$F = \{f_{i,j,j_1,j_2}\}_{i,j,k,l \in [d]} = \{(Aa)_{i,j_1}(B^{-1})_{j_2,j})\}_{i,j,j_1,j_2 \in [d]},$$
$$R' = Aa \cdot M^x \cdot B^{-1}.$$

Arranging F, we obtain

$$F' = (Aa)^\top \otimes (B^{-1}) \in M(\mathbb{F}, d^2).$$

From the definition of ρ, Aa and B^{-1} is invertible. Therefore, $F' = (Aa)^\top \otimes (B^{-1})$ has rank d^2. Hence, the eavesdropper can compute $\mathrm{vec}(M^x) = F'^{-1} \cdot \mathrm{vec}(R')$ and obtain M^x.

Remark 3.1. From the slides of Accardi's talk [Acc11] and [July 2011, private communication], they already noticed that the AIRO-T1 protocol is vulnerable as the above attack has shown.

4 The AIRO-T2 Protocol

In the AIRO-T1 protocol, the problem arises from $\rho \circ \pi_1$ and F. As already noted, they were aware of the danger in the above and proposed another way to remove the vulnerability, which is the AIRO-T2 protocol in [Acc11].

4.1 The AIRO-T2 Protocol

In the AIRO-T2 protocol, $\mathcal{I}$ sends $(F, AbB^{-1} + C, n)$ as $\rho \circ \pi_1 \circ \pi_2$. Accardi et al. set

$$F = \{f_{i,j,j_1,j_2}\} = \{(AaPW)_{i,j_1}(W^{-1}P^{-1}B^{-1})_{j_2,j}\},$$

where W is a random invertible element commutative with any element in $\mathbb{S}_G$. By using these, the responder can compute the mapping

$$G^x \in \mathbb{S}_G \mapsto AaP \cdot G^{nx} \cdot P^{-1}B^{-1} + AbB^{-1} + C$$
$$= \rho \circ \pi_1 \circ \pi_2(G^x) \in M(\mathbb{F}, d).$$

Formally, the AIRO-T2 protocol is described as follows:

- $\mathcal{I}, \mathcal{R}$: Both parties share the parameters, $\mathbb{F}, d, G$.
- $\mathcal{I} \to \mathcal{R}$: Choose $\pi_0, \pi_1, \pi_2, \rho$ by generating $A_i, B_i, C \in \mathbb{S}$, $a, b, \in \mathbb{F}$, $A, B, P, W \in \mathrm{GL}(\mathbb{F}, d)$ and $n \in \mathbb{N}$ randomly. Send $\pi_0 \circ \pi_1$, $(F, AbB^{-1} + C, n)$ as $\rho \circ \pi_1 \circ \pi_2$, and $M = \pi_2(G)$.
- $\mathcal{R} \to \mathcal{I}$: Choose $x \leftarrow \mathbb{N}$. Send $R = \rho \circ \pi_1 \circ \pi_2(G^x)$.
- I: Compute $K = \pi_0 \circ \rho^{-1}(R)$ $(= \pi_0 \circ \pi_1 \circ \pi_2(G^x))$.
- R: Compute $K = \pi_0 \circ \pi_1(M^x)$ $(= \pi_0 \circ \pi_1 \circ \pi_2(G^x))$.

4.2 An Attack

Here, we show an attack against the AIRO-T2 protocol, which is essentially the same as Accardi's [July 2011, private communication].

For ease of notation, we set $S = AaPW$ and $T = W^{-1}P^{-1}B^{-1}$, which are in $\mathrm{GL}(\mathbb{F}, d)$. We also set $\bar{G} = G^n$. We notice that

$$R = S \cdot \bar{G}^x \cdot T + AbB^{-1} + C.$$

Since an eavesdropper has $F = \{S_{i,j_1}T_{j_2,j}\}$ and $AbB^{-1} + C$, it can retrieve $\bar{G}^x$ from R, F, and $AbB^{-1} + C$ as in the previous attack. Now, it has G from the public parameter, $\pi_0 \circ \pi_1$, n, $M = \pi_2(G) = P\bar{G}P^{-1}$ from the transmission from $\mathcal{I}$ to $\mathcal{R}$, and $\bar{G}$ and $\bar{G}^x$. To generate $K = \pi_0 \circ \pi_1(M^x)$ as $\mathcal{R}$ does, it suffices to compute $M^x = P\bar{G}^xP^{-1}$.

Now, the problem is finding $M^x = P\bar{G}^xP^{-1}$ given $M = P\bar{G}P^{-1}$, $\bar{G}$, and $\bar{G}^x$. The following algorithm is inspired by an attack by Rasslan and Youssef [RY11] whose brief review appears in Appendix A.

1. Input is $M = P\bar{G}P^{-1}$, $\bar{G}$, and $\bar{G}^x$.
2. Compute $c_0, \ldots, c_{d-1} \in \mathbb{F}$ such that $\bar{G}^x = \sum_{i=0}^{d-1} c_i\bar{G}^i$ using vectorization and the standard linear algebra.
3. Output $\sum_{i=0}^{d-1} c_iM^i$ as $M^x = P\bar{G}^xP^{-1}$.

Theorem 4.1. *The above algorithm finds $M^x = P\bar{G}^xP^{-1}$.*

Proof. From the claim below, it holds that

$$\{\bar{G}^i : i \in \mathbb{N}\} \subseteq \{\textstyle\sum_{i=0}^{d-1} c_i\bar{G}^i : c_i \in \mathbb{F}\}.$$

So, Step 2 outputs $c_0, \ldots, c_{d-1} \in \mathbb{F}$ such that $\bar{G}^x = \sum_{i=0}^{d-1} c_i\bar{G}^i$. From the above, we have that

$$M^x = P\bar{G}^xP^{-1} = P\left(\sum_{i=0}^{d-1} c_i\bar{G}^i\right)P^{-1} = \sum_{i=0}^{d-1} c_iP\bar{G}^iP^{-1} = \sum_{i=0}^{d-1} c_iM^i$$

in Step 3 as we wanted. □

Claim 4.2. *Let $\mathbb{F}$ be a finite field and let d be a positive integer. For any $\bar{G} \in M(\mathbb{F}, d)$ we have*

$$\{\bar{G}^i : i \in \mathbb{N}\} \subseteq \{\textstyle\sum_{i=0}^{d-1} c_i\bar{G}^i : c_i \in \mathbb{F}\}.$$

Proof of claim. To verify the inclusion, we use the Hamilton-Cayley theorem, which says that for any matrix $\bar{G} \in M(\mathbb{F}, d)$, $p_{\bar{G}}(\bar{G}) = O$, where $p_{\bar{G}}(\lambda)$ is the characteristic polynomial of $\bar{G}$. Since $\mathbb{F}$ is a finite field, so, $p_{\bar{G}}(\lambda)$ is in $\mathbb{F}[\lambda]$. In addition, its degree is at most d. So that we can write $p_{\bar{G}}(\lambda) = p_0 + p_1\lambda + \cdots + p_{d-1}\lambda^{d-1} + \lambda^d$ and we have that

$$\bar{G}^d = -(p_{d-1}\bar{G}^{d-1} + \cdots + p_1\bar{G} + p_0I).$$

By induction, for any natural number k, there exist $c_0, \ldots, c_{d-1} \in \mathbb{F}$ such that

$$\bar{G}^k = c_{d-1}\bar{G}^{d-1} + \cdots + c_1\bar{G} + c_0I.$$

□

References

[Acc11] Luigi Accardi. Algoritmi fortemente asimmetrici per la distribuzione pubblica di chiavi crittografiche (PKD). A seminar at Università di Roma "Tor Vergata", April 2011. Slides are available at `http://people.dii.uniroma2.it/OR%20Group/AlgoCol.html`.

[AIRO11a] Luigi Accardi, Satoshi Iriyama, Massimo Regoli, and Masanori Ohya. Strongly asymmetric PKD algorithms — an implementation using the matrix model. Technical Report ISEC2011-21, IEICE, 2011.

[AIRO11b] Luigi Accardi, Satoshi Iriyama, Massimo Regoli, and Masanori Ohya. Strongly asymmetric public key agreement algorithms. Technical Report ISEC2011-20, IEICE, 2011.

[BG99] Simon R. Blackburn and Steven Galbraith. Cryptanalysis of two cryptosystems based on group actions. In Kwok-Yan Lam, Eiji Okamoto, and Chaoping Xing, editors, *ASIACRYPT '99*, volume 1716 of *Lecture Notes in Computer Science*, pages 52–61. Springer-Verlag, 1999.

[MN79] Jan R. Magnus and H. Neudecker. The commutation matrix: Some properties and applictions. *Annals of Statistics*, 7(2):381–394, 1979.

[PZZ07] Shi-Hui Pei, Yong-Zhe Zhao, and Hong-Wei Zhao. Construct public key encryption scheme using ergodic matrices over GF(2). In Jin-Yi Cai, S. Barry Cooper, and Hong Zhu, editors, *TAMC 2007*, volume 4484 of *Lecture Notes in Computer Science*, pages 181–188. Springer-Verlag, 2007.

[RY11] Mohamed Rasslan and Amr Youssef. Cryptanalysis of a public key encryption scheme using ergodic matrices. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E94-A(2):853–854, 2011.

[Zum08] Jens Zumbrägel. *Public-key cryptography based on simple semirings*. PhD thesis, Universität Zürich, December 2008.

A An Attack by Rasslan and Youssef

We briefly review the target [PZZ07] and an attack by Rasslan and Youssef [RY11].

The target: Pei, Zhao, and Zhao [PZZ07] proposed public-key encryption scheme by using $M(\mathbb{F}_2, d)$. Roughly speaking, $\mathcal{I}$ chooses $Q_1, Q_2, G \leftarrow M(F_2, d)$, $s, t \leftarrow [2^d]$, and sends $Q_1, Q_2, G, M = Q_1^s \cdot G \cdot Q_2^t \in M(\mathbb{F}_2, d)$. (The orbits of Q_1 and Q_2 should be long.) $\mathcal{R}$ randomly chooses $k, l \leftarrow [2^d]$ and sends $R = Q_1^k \cdot G \cdot Q_1^l$. Both party shares key $K = Q_1^{s+k}GQ_2^{t+l} = Q_1^s \cdot R \cdot Q_2t = Q_1^k \cdot M \cdot Q_2^l$.

The attack: Rasslan and Youssef [RY11] analysed the public-key encryption in the above. If an eavesdropper can compute the mapping $X \mapsto Q_1^s X Q_2^t$ from transmission, then it can compute the shared key, $K = Q_1^s \cdot R \cdot Q_2^t$. To retrieve the mapping, Rasslan and Youssef gave the following algorithm. For $i = 1, \ldots, d^2$, generates random integers $k_i, l_i \in [2^d]$ and compute $B_i = Q_1^{k_i} \cdot Q_1^s G Q_2^t \cdot Q_2^{l_i} = Q_1^s (Q_1^{k_i} G Q_2^{l_i}) Q_2^t$ and $C_i = Q_1^{k_i} G Q_2^{l_i}$. From our perspective, this is interpreted as, for $i = 1, \ldots, d^2$

$$\mathrm{vec}(B_i) = \mathrm{vec}(Q_1^s \cdot C_i \cdot Q_2^t) = \mathrm{vec}(C_i) \cdot ((Q_1^s)^\top \otimes Q_2^t).$$

Let

$$B = \begin{bmatrix} \mathrm{vec}(B_1) \\ \vdots \\ \mathrm{vec}(B_{d^2}) \end{bmatrix}, C = \begin{bmatrix} \mathrm{vec}(C_1) \\ \vdots \\ \mathrm{vec}(C_{d^2}) \end{bmatrix}.$$

Combining the above, we have

$$B = C \cdot ((Q_1^s)^\top \otimes Q_2^t).$$

They insisted that C is full-rank with high probability without proof. If so, we can compute $(Q_1^s)^\top \otimes Q_2^t = C^{-1} \cdot B$ and we are able to compute the mapping $X \mapsto Q_1^s X Q_2^t$ by using $(Q_1^s)^\top \otimes Q_2^t$.