Journal of Mathematical Sciences, Vol. 195, No. 4, December, 2013

CATEGORICAL INTERPRETATIONS OF SOME KEY AGREEMENT PROTOCOLS

N. Inassaridze, T. Kandelaki, and M. Ladra UDC 519.72

Abstract. We give interpretations of some known key agreement protocols in the framework of category theory and in this way we propose a method of constructing of many new key agreement protocols.

CONTENTS

1. Introduction

Key agreement is one of the fundamental cryptographic primitives after encryption and digital signature. Key agreement protocols (KAPs) allow two or more parties to exchange information among themselves over an adversarially controlled insecure network and agree upon a common session key, which may be used for later secure communication among the parties. Thus, secure KAPs serve as a basic building block for constructing secure, complex, higher level cryptographic protocols. The first pioneering work for key agreement is the Diffie–Hellman protocol given in their seminal paper [2] that invents the public key cryptography and revolutionizes the field of modern cryptography. In [2], a two-party key agreement protocol was proposed. There have been many attempts to provide authentic key agreement protocols based on the Diffie–Hellman protocol (see [3, 6, 7, 9]). In the last few years some effort has been made to construct KAP using hard problems in infinite noncommutative groups. Here we only mention the idea based on conjugacy search problems that were reckoned as potentially hard problems for construction of one-way functions (see [1, 4]). To realize the proposed algorithms, the main attempts were directed to suitable platform group selection. Recently in [8] the KAP was constructed using matrix power functions based on matrix ring action on some matrix set and generalizing the Diffie–Hellman KAP. It has been suggested that the main advantage of the proposed KAP is considerable fast computations and avoidance of arithmetic operations with long integers. The aim of this work is to suggest a general scheme of constructing KAPs using the category theory. We assume the reader is familiar with categories (we refer to the classical book of MacLane [5] for the background in category theory). Based on the structure of categories, we present the above mentioned KAPs as very particular cases of our categorical KAPs. Working new examples of our categorical KAPs will be given in subsequent papers.

2. Key Agreement Protocols Related to Categories

In this section, we define KAPs that arise from the structure of categories.

Translated from Sovremennaya Matematika i Ee Prilozheniya (Contemporary Mathematics and Its Applications), Vol. 83, Modern Algebra and Its Applications, 2012.

2.1. KAPs based on categories. Let $\mathcal{C}$ be a (nonempty) category and let A and B be objects of $\mathcal{C}$ such that $\mathrm{Hom}(A,B) \neq \varnothing$. We assume that the set $\mathrm{Hom}(A,B)$ is a set of possible keys, while $\mathrm{Hom}(A,A)$ and $\mathrm{Hom}(B,B)$ are monoids that can be used by Alice and Bob, respectively, for actions on $\mathrm{Hom}(A,B)$ if they wish to create a shared key. According to the structure of the category $\mathcal{C}$, Alice is able to act on the set of possible keys using the right action of $\mathrm{Hom}(A,A)$ on $\mathrm{Hom}(A,B)$. Similarly, Bob is able to act on the set of possible keys using the left action of $\mathrm{Hom}(B,B)$ on $\mathrm{Hom}(A,B)$. Let g be a publicly known element of the set $\mathrm{Hom}(A,B)$. Then, for creating a shared key, Alice and Bob can proceed as follows:

(1) Alice selects at random an element $f \in \mathrm{Hom}(A,A)$ and computes the composition $g \cdot f$ and sends it to Bob;
(2) Bob selects at random an element $h \in \mathrm{Hom}(B,B)$ and computes the composition $h \cdot g$ and sends it to Alice;
(3) Alice computes $k_a = (h \cdot g) \cdot f$, while Bob computes $k_b = h \cdot (g \cdot f)$;
(4) since $(h \cdot g) \cdot f = h \cdot (g \cdot f)$, the shared key is $k = k_a = k_b \in \mathrm{Hom}(A,B)$.

This protocol, based on the structure of the category $\mathcal{C}$, is called the categorical key agreement protocol (CKAP).

2.2. General form of KAPs based on enriched categories. In this section, we give another scheme of KAPs induced by a structure of a category, but which is enriched over the category of Abelian groups, i.e., a category whose morphism sets are Abelian groups satisfying some axioms (see [5]). This construction generalizes the KAPs given in Sec. 2.1 and motivated by some known KAPs. Namely, our approach makes it possible to interpret many known KAPs as particular cases of our construction. Let $\mathcal{D}$ be a (nonempty) enriched category over the category of Abelian groups. Clearly, this means that for any objects A and B in this category, $\mathrm{Hom}(A,A)$ and $\mathrm{Hom}(B,B)$ are unital rings, $\mathrm{Hom}(A,B)$ is an Abelian group, and the composition of morphisms in $\mathcal{D}$ is bilinear. Let A and B be objects of $\mathcal{D}$ such that $\mathrm{Hom}(A,B) \neq \varnothing$. Let m and n be natural numbers, $\mathcal{A}_A$ and $\mathcal{B}_A$ be commuting subrings of the $(n \times n)$-matrix ring $M_n\big(\mathrm{Hom}(A,A)\big)$, and $\mathcal{A}_B$ and $\mathcal{B}_B$ be commuting subrings of the $(m \times m)$-matrix ring $M_m\big(\mathrm{Hom}(B,B)\big)$. Let φ be a publicly known $(m \times n)$-matrix over the Abelian group $\mathrm{Hom}(A,B)$. If Alice and Bob wish to create a common secret key, they can proceed as follows:

(1) Alice selects at random matrices $\psi_a \in \mathcal{A}_A$ and $\omega_a \in \mathcal{A}_B$, computes the product of matrices $\omega_a \cdot \varphi \cdot \psi_a$, and sends it to Bob;
(2) Bob selects at random matrices $\psi_b \in \mathcal{B}_A$ and $\omega_b \in \mathcal{B}_B$, computes the product of matrices $\omega_b \cdot \varphi \cdot \psi_b$, and sends it to Alice;
(3) Alice computes $k_a = \omega_a \cdot \omega_b \cdot \varphi \cdot \psi_b \cdot \psi_a$, while Bob computes $k_b = \omega_b \cdot \omega_a \cdot \varphi \cdot \psi_a \cdot \psi_b$;
(4) since $\omega_a \cdot \omega_b = \omega_b \cdot \omega_a$ and $\psi_b \cdot \psi_a = \psi_a \cdot \psi_b$, the shared secret key is the $(m \times n)$-matrix $k = k_a = k_b$ over the Abelian group $\mathrm{Hom}(A,B)$.

This protocol is called the enriched categorical key agreement protocol (ECKAP). The following assertion relates the two categorical KAPs presented in this section.

Theorem 2.1. *There is a universal faithful functor T from the category of categories to the category of enriched categories over the category of Abelian groups. According to this correspondence, any CKAP related to a category $\mathcal{C}$ can be interpreted as an ECKAP related to the enriched category $T(\mathcal{C})$.*

Proof. We just construct the functor T and omit the proof of its universality since it directly follows from the construction. In fact, for any category $\mathcal{C}$ define the category $T(\mathcal{C})$ as follows: its objects class coincides with the objects class of $\mathcal{C}$, while $\mathrm{Hom}_{T(\mathcal{C})}(A,B)$ is the free Abelian group generated by the set $\mathrm{Hom}_{\mathcal{C}}(A,B)$ for any $A, B \in T(\mathcal{C})$. The composition of morphisms in $T(\mathcal{C})$ is obviously induced

by the composition of morphisms in $\mathcal{C}$. Then it is easy to verify that $\mathrm{Hom}_{T(\mathcal{C})}(A, A)$, $A \in T(\mathcal{C})$, is a unital ring, the composition is bilinear, and all axioms of the enriched category are satisfied. Hence the category $T(\mathcal{C})$ is enriched over the category of Abelian groups. Given a category $\mathcal{C}$, one can obtain its corresponding CKAP as the ECKAP of the enriched category $T(\mathcal{C})$ by assuming that $m = n = 1$ and $\mathcal{B}_A$ and $\mathcal{A}_B$ are subrings of $M_n\big(\mathrm{Hom}(A, A)\big)$ and $M_m\big(\mathrm{Hom}(B, B)\big)$ generated by the unital matrices, respectively. □

Remark 2.2. In our constructions, one can successfully use an enriched category over any symmetric monoidal category, for example, over the category of Abelian monoids (see Theorem 3.3).

2.3. Security problem of CKAPs and ECKAPs. Assume that any KAP must be secure up to solving a certain mathematical problem in a reasonable length of time. One can see that CKAPs and ECKAPs are based on the conjecture that a function defined by the composition of morphisms in a category is a one-way function in general. We suggest that the security of CKAPs and ECKAPs depends on a concrete model of a given category, i.e., the cardinality of "Hom-sets" and the nontriviality of the morphism composition. We also would like to mention that the security of our categorical KAPs is not less than the security of the Diffie–Hellman KAP (see [2]) and Ko–Lee–Cheon–Han–Kang–Park KAP (see [4]), since they are particular cases of our KAPs (see Sec. 3). Further discussion on the security problems will be developed in subsequent papers where the concrete implementations of our KAPs are given.

3. Interpretations of Some Well-Known KAPs

In this section, we show that some of well-known KAPs are particular cases of our general categorical KAPs.

3.1. Diffie–Hellman KAP as a CKAP. The Diffie–Hellman key agreement protocol is defined in [2]. It has the following form. Let G be a cyclic group and g a generator of G, where both g and its order s are publicly known. If Alice and Bob wish to create a shared key, they can proceed as follows:

(1) Alice selects uniformly at random an integer $m \in [2, s-1]$, computes g^m, and sends it to Bob;
(2) Bob selects uniformly at random an integer $n \in [2, s-1]$, computes g^n, and sends it to Alice;
(3) Alice computes $k_m = (g^n)^m$, while Bob computes $k_n = (g^m)^n$;
(4) the shared key is thus $k = k_m = k_n \in G$.

Theorem 3.1. *The Diffie–Hellman KAP is a CKAP based on a certainly constructed category. Moreover, one can interpret it as an ECKAP.*

Proof. Let us construct a category $\mathcal{C}$ as follows. Let $\mathcal{C}$ have only two objects A and B. Let the morphism sets be $\mathrm{Hom}(A, A) = \mathbb{N}$, $\mathrm{Hom}(B, B) = \mathbb{N}$, $\mathrm{Hom}(A, B) = G$, and $\mathrm{Hom}(B, A) = \varnothing$, where $\mathbb{N}$ is the Abelian monoid of natural numbers with respect to usual product. Finally, let the composition of morphisms be defined by the formulas

$$n \cdot g = g^n \quad \text{and} \quad g \cdot m = g^m, \quad m, n \in \mathbb{N},\ g \in G.$$

It is easy to see that the CKAP that arises from the structure of the so-defined category $\mathcal{C}$ is exactly the Diffie–Hellman KAP. Owing to Theorem 2.1, the rest of the assertion follows. □

3.2. Ko–Lee–Cheon–Han–Kang–Park KAP as a CKAP. Recall the Ko–Lee–Cheon–Han–Kang–Park key agreement protocol (briefly, the Ko KAP) given in [4]. Let G be a non-Abelian group and H_A and H_B be commuting subgroups of it. Let g be a publicly known element of G. If Alice and Bob wish to create a common secret key, they can proceed as follows:

(1) Alice selects at random an element $a \in H_A$, computes ${}^a g = aga^{-1}$, and sends it to Bob;

(2) Bob selects at random an element $b \in H_B$, computes ${}^b g = bgb^{-1}$, and sends it to Alice;
(3) Alice computes $k_a = {}^a({}^b g)$, while Bob computes $k_b = {}^b({}^a g)$;
(4) the common secret key is $k = k_a = k_b \in G$.

Theorem 3.2. *The Ko KAP is a CKAP that arises from a certainly constructed category. Moreover, one can interpret it as an ECKAP.*

Proof. Let us construct a category $\mathcal{C}$ as follows. Let $\mathcal{C}$ have only two objects A and B. Let the morphism sets be $\mathrm{Hom}(A, A) = H_A$, $\mathrm{Hom}(B, B) = H_B$, $\mathrm{Hom}(A, B) = G$, and $\mathrm{Hom}(B, A) = \varnothing$. Finally, let the composition of morphisms be defined by the equalities

$$a \cdot a' = a'a, \quad b \cdot b' = bb', \quad g \cdot a = aga^{-1} \quad \text{and} \quad b \cdot g = bgb^{-1}$$

for $a, a' \in \mathrm{Hom}(A, A)$, $b, b' \in \mathrm{Hom}(B, B)$, and $g \in \mathrm{Hom}(A, B)$. It is clear that the CKAP that arises from the category $\mathcal{C}$ is exactly the Ko KAP. Now, using again Theorem 2.1, we complete the proof. □

3.3. Sakalauskas–Listopadskis–Tvarijonas KAP as an ECKAP. In [8], Sakalauskas, Listopadskis, and Tvarijonas defined a KAP (briefly called the Sakalauskas KAP) based on matrix power functions. Now we recall it but in a slightly modified form. Let $\mathcal{S}$ be a semiring and $\mathcal{M}$ be a $\mathcal{S}$-semibimodule, i.e., there exist bilinear right and left actions of $\mathcal{S}$ on the Abelian monoid $\mathcal{M}$ satisfying the following associative law:

$$(lm)r = l(mr), \quad l, r \in \mathcal{S},\ m \in \mathcal{M}.$$

Let k be a natural number and let $M_k(\mathcal{S})$ and $M_k(\mathcal{M})$ denote a $(k \times k)$-matrix semiring over $\mathcal{S}$ and a $(k \times k)$-matrix Abelian monoid over $\mathcal{M}$, respectively. It is well known that $M_k(\mathcal{M})$ is a $M_k(\mathcal{S})$-semibimodule with respect to the naturally induced right and left actions by the rule of standard matrix multiplication. Let φ be a publicly known $(k \times k)$-matrix in $M_k(\mathcal{M})$, and $\mathcal{A}_A$ and $\mathcal{A}_B$ be two subsemirings of commuting matrices in $M_k(\mathcal{S})$. If Alice and Bob wish to create a common secret key, they can proceed as follows:

(1) Alice selects at random secret matrices $\psi_a \in \mathcal{A}_A$ and $\omega_a \in \mathcal{A}_B$, computes the product of matrices $\omega_a \cdot \varphi \cdot \psi_a$, and sends it to Bob;
(2) Bob selects at random secret matrices $\psi_b \in \mathcal{A}_A$ and $\omega_b \in \mathcal{A}_B$, computes the product of matrices $\omega_b \cdot \varphi \cdot \psi_b$, and sends it to Alice;
(3) both parties compute the following common secret (key) matrix k:

$$k = \omega_a \cdot \omega_b \cdot \varphi \cdot \psi_b \cdot \psi_a = \omega_b \cdot \omega_a \cdot \varphi \cdot \psi_a \cdot \psi_b.$$

Theorem 3.3. *The Sakalauskas KAP is an ECKAP that arises from a certainly constructed enriched category over the category of Abelian monoids.*

Proof. According to the structure of $\mathcal{S}$-semibimodule $\mathcal{M}$, one constructs the enriched category over the category of Abelian monoids $\mathcal{D}$ with two objects A and B and the following "Hom-objects":

$$\mathrm{Hom}(A, A) = \mathcal{S}, \quad \mathrm{Hom}(B, B) = \mathcal{S}, \quad \mathrm{Hom}(A, B) = \mathcal{M}, \quad \mathrm{Hom}(B, A) = \varnothing,$$

while the composition is defined by the right and left actions of $\mathcal{S}$ on $\mathcal{M}$. Now, it is obvious that the ECKAP that arises from the enriched category $\mathcal{D}$ coincides with the Sakalauskas KAP. □

4. Categorical Multi-Party KAP

This section suggests multi-party KAP based on the structure of a category, hence showing the advantage of the categorical approach to constructing easily multi-party KAPs. Further investigation of our categorical multi-party KAP and its working examples will appear in our subsequent papers. Assume that there is a set $S = \{A_1, A_2, \ldots, A_n\}$ of n users. If they wish to agree a common secret key and for that to use open insecure channels, they can proceed as follows.

Step 1. Choose an order in S, i.e., $S = \big(A_1, A_2, \ldots, A_n\big)$.

Step 2. A category $\mathcal{C}$ is public. For each user A_i, $1 \le i \le n$, is chosen an object $C_i \in \mathcal{C}$ publicly and $(n-1)$ elements $\{g_1, \ldots, g_{n-1}\}$ such that $g_i \in \mathrm{Hom}(C_i, C_{i+1})$.

Step 3. Any user A_i, $1 \le i \le n$, chooses randomly an element $f_i \in \mathrm{Hom}(C_i, C_i)$ and computes

$$\begin{aligned} &g_i f_i && && \text{for} \quad i = 1, \\ &f_i g_{i-1} && && \text{for} \quad i = n, \\ &f_i g_{i-1} \quad \text{and} && g_i f_i \quad \text{for} \quad 1 < i < n. \end{aligned}$$

Then any user A_i sends $g_i f_i$ to any other user A_j for $j > i$ and sends $f_i g_{i-1}$ to any other user A_j for $j < i$.

Step 4. Owing to the associative law of morphism composition in the category $\mathcal{C}$, any user A_i computes

$$k_i = (f_n g_{n-1}) \cdots (f_{i+1} g_i) f_i (g_{i-1} f_{i-1}) \cdots (g_1 f_1) = f_n g_{n-1} \cdots f_{i+1} g_i f_i g_{i-1} f_{i-1} \cdots g_1 f_1 = k$$

and obtain a common element $k \in \mathrm{Hom}(C_1, C_n)$.

Acknowledgements. The first and third authors were partially supported by Ministerio de Ciencia e Innovación (European FEDER support included), grant MTM2009-14464-C02, and by Xunta de Galicia, grant Incite 09 207 215 PR.

REFERENCES

1. I. Anshel, M. Anshel, and D. Goldfeld, "An algebraic method for public-key cryptography," *Math. Res. Lett.*, **6**, 287–291 (1999).
2. W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, **22**, 644–654 (1976).
3. W. Diffie, P. C. van Oorschot, and M. J. Wiener, "Authentication and authenticated key exchanges," *Des. Codes Cryptogr.*, **2**, 107–125 (1992).
4. K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. S. Kang, and C. Park, "New public-key cryptosystem using braid group," in: *Advances in Cryptology, CRYPTO* 2000 (M. Bellare, ed.), Lect. Notes Comput. Sci., **1880**, Springer-Verlag (2000), pp. 166–183.
5. S. MacLane, *Categories for the Working Mathematician*, Grad. Texts Math., **5**, Springer-Verlag, New York–Berlin (1971).
6. T. Matsumoto, Y. Takashima, and H. Imai, "On seeking smart public-key distribution systems," *Trans. IEICE Jpn.*, **E69**, No. 2, 99–106 (1986).
7. A. Menezes, M. Qu, and S. Vanstone, "Some new key agreement protocols providing implicit authentication," *Proc. 2nd Workshop on Selected Areas in Cryptography* (SAC '95), Springer-Verlag (1995), pp. 22–32.
8. E. Sakalauskas, N. Listopadskis, and P. Tvarijonas, "Key agreement protocol (KAP) based on matrix power functions," in: *Adv. Stud. in Software and Knowledge Engineering* (2008), pp. 92–96.
9. Y. Yacobi, "A key distribution 'Paradox'," in: *Advances in Cryptology, CRYPTO* '90 (A. J. Menezes and S. A. Vanstone, eds.), Lect. Notes Comput. Sci., **537**, Springer-Verlag (1991), pp. 268–273.

N. Inassaridze
Departamento de Matemática Aplicada I, Universidad de Vigo, Pontevedra, Spain;
Tbilisi Center for Mathematical Sciences, Tbilisi, Georgia;
A. Razmadze Mathematical Institute, Tbilisi, Georgia
E-mail: niko.inas@gmail.com

T. Kandelaki
Tbilisi Center for Mathematical Sciences, Tbilisi, Georgia;
A. Razmadze Mathematical Institute, Tbilisi, Georgia
E-mail: kandel@rmi.ge; tam.kandel@gmail.com
M. Ladra
Departamento de Álgebra, Facultad de Matemáticas,
Universidad de Santiago de Compostela, Spain
E-mail: manuel.ladra@gmail.com