Geometric Key Establishment

9/12/2004

Arkady Berenstein[i] and Leon Chernyak[ii]

Abstract

We propose a new class of key establishment schemes which are based on geometric generalizations of the classical Diffie-Hellman. The simplest of our schemes – based on the geometry of the unit circle – uses only multiplication of rational numbers by integers and addition of rational numbers in its key creation. Its first computer implementation works significantly faster than all known implementations of Diffie-Hellman. Preliminary estimations show that our schemes are resistant to attacks. This resistance follows the pattern of the discrete logarithm problem and hardness of multidimensional lattice problems.

Introduction

In this paper we propose a new class of key establishment schemes which we refer to as Geometric Key Establishment (GKE). Similarly to Diffie-Hellman ([5]), the GKE schemes do not assume that communicating parties share any kind of secret information prior to the act of key creation and distribution.

The GKE schemes are based on the mathematical concept of semigroup action and its modification – commuting double action. Cryptographic applications of the semigroup actions are well-known: Diffie-Hellman schemes are based on actions of the semigroup of integers (under multiplication) on finite groups. More recent applications include two-sided multiplications in semigroups and groups ([8]), actions of semigroups of square integer matrices on finite commutative groups ([7]) and actions of braid semigroups on braid groups ([2]).[1]

Although general commuting double actions seem to be well-known in mathematics, we are unaware of any application of this concept in key establishment protocols.[2] In the present work we construct two geometric key establishment schemes (GKE I and GKE II) which are based primarily on the concept.

Typically, Diffie-Hellman-like schemes involve time-consuming exponentiation procedures in finite fields or finite groups. Unlike this, GKE I and GKE II do not use any exponentiation. We bypassed exponentiation by replacing the semigroup actions on finite groups with actions (or commuting double actions) on infinite and even continuous groups. In particular, the simplest of our schemes is based on the action of the semigroup of integer square matrices on the unit cube, and, by design, uses only multiplication of real numbers by integers and addition of real numbers in its key creation.

First computer implementations of the cube-based schemes work with a much higher speed than all known implementations of Diffie-Hellman. More precisely, the

[1] An approach not based on Diffie-Hellman has been suggested by I. Anshel, M. Anshel, and D. Goldfeld in [1] and [3].

[2] The approach developed in [8] utilizes a particular case of two-sided action. The limitation of this approach consists in the requirement that the involved semigroups are commutative.

running time of GKE I (resp. GKE II) is proportional to N^2 (resp. $N^{3/2}$) with the assumption that multiplication of two numbers takes a constant time, where N is the size of the input.

Preliminary estimations show that GKE I and GKE II are resistant to basic attacks. This resistance follows the pattern of the discrete logarithm problem. A more detailed study of GKE security is a work [4] joint with Professor Itkis of Boston University.

As we said above, our schemes rely on infinite geometric objects or, more precisely, on compact connected topological groups such as the unit circle or an *n*-dimensional torus. Of course, the schemes, as based on infinite geometric objects, are *ideal* in that sense that no *real* computing device can create or communicate keys as points of a geometric continuum. In order to implement GKE in a real device, we developed (based on the ordinary rounding of real numbers) a procedure of *discretization* of our ideal, continuous schemes. This procedure allows for creating an infinite family of *real* key establishment protocols. These real protocols seem to be cryptographically sound, which fact is by itself very inspiring.

Having been encouraged by obtaining a rich family of discretizations for GKE, we proceeded to generalization of the relationship between ideal and real key establishment schemes. As a result, we introduced a general concept of Rounded Key Establishment (RKE). This latter concept consists of an ideal continuous scheme and a family of its discretizations. One of surprising results of this generalization is a rigorous mathematical definition of key establishment, in which all existing Diffie-Hellman-like schemes fit perfectly. We have not been able to find any reference to similarly rigorous mathematical definition of key establishment in the literature.

We hope that, in addition to GKE I and GKE II, our concept of RKE will bring new interesting examples of key establishment schemes.

The paper is organized as follows:

In *Section* 1 we introduce key establishment paradigms based on commuting double actions. Our main examples include all schemes based on semigroup and ring actions and, in particular, Diffie-Hellman scheme and its generalizations. Our examples will be used in the following sections for constructing our GKE I and GKE II schemes.

Section 2 is devoted to introduction and study of our first main example – Geometric Key Establishment I (GKE I). We start with a description of an ideal GKE I and then construct a family of its discretizations. The main result of the section is Theorem 2.2, which asserts that these discretizations bring about a family of real key establishment protocols. We conclude the section with a numerical example demonstrating how the real GKE I protocols work.

Section 3 is devoted to introduction and study of our second main example – Geometric Key Establishment II (GKE II). The section is structured similarly to Section 2. We start with a description of an ideal GKE II and then construct a family of its discretizations. The main result of the section is Theorem 3.2, which asserts that these discretizations bring about a family of real key establishment protocols. We conclude the section with a numerical example demonstrating how the real GKE II protocols work.

In *Appendix A* we develop a conceptual framework for rounded key establishment (RKE). The basic key establishment scheme (Definition A.1) is quite trivial and, apparently, is well known (although we have been unable to find appropriate references). However, having been written in the set-theoretic language, it allows for a simple conceptual definition of RKE. This approach is common in modern mathematics: once an object is defined set-theoretically, it can further be enriched topologically, algebraically, and geometrically.

Appendix B consists of the proofs of main results – Theorem 2.2 and Theorem 3.2.

Acknowledgements. The authors express their gratitude to Igor Mendelev for invaluable help in implementation of the first prototype of GKE and for performing the comparative analysis of GKE prototype with other key establishment systems. Our thanks are due to Professor Itkis of Boston University for extremely helpful comments and remarks on this manuscript. The authors wish to thank Professor Michael Anshel of City College of New York for very helpful references in the field of the semigroup-based cryptography. We would like to express our gratitude to Professor Shpilrain for giving us the opportunity to present this work at the "Algebraic Cryptography" section of Canadian Mathematical Society conference held in December 2004.

Section 1. Key establishment schemes based on commuting double actions

In this section we introduce a class of key establishment schemes which we refer to as *commuting double action* schemes. This class of schemes is based on the mathematical concept of *commuting double action*.

Definition 1.1. Let A, B, and X be sets. A quadruple of maps $A\times X\to X$, $X\times A\to X$ and $B\times X\to X$, $X\times B\to X$ (denoted respectively as: $(\boldsymbol{a}, \boldsymbol{x})\to\boldsymbol{a}(\boldsymbol{x})$, $(\boldsymbol{x}, \boldsymbol{a})\to(\boldsymbol{x})\boldsymbol{a}$ and $(\boldsymbol{b}, \boldsymbol{x})\to\boldsymbol{b}(\boldsymbol{x})$, $(\boldsymbol{x}, \boldsymbol{b})\to(\boldsymbol{x})\boldsymbol{b}$) is a *commuting double action* of A and B on X if:

(1.1) $$(\boldsymbol{a}(\boldsymbol{x}))\boldsymbol{b} = (\boldsymbol{b}(\boldsymbol{x}))\boldsymbol{a}$$

for any $\boldsymbol{x}\in X$ and any $\boldsymbol{a} \in A$, $\boldsymbol{b}\in B$.

Commuting double action key establishment scheme

Setup (non-secret parameters)

- Sets A, B, and X
- a commuting double action $A\times X\to X$, $X\times A\to X$ and $B\times X\to X$, $X\times B\to X$

Protocol

- *Alice* and *Bob*: choose a non-secret element $\boldsymbol{x}\in X$
- *Alice*: choose a secret element $\boldsymbol{a}\in A$
- *Bob*: choose a secret element $\boldsymbol{b}\in B$
- *Alice*→*Bob*: $m_A=\boldsymbol{a}(\boldsymbol{x})$
- *Bob*: compute $S_B= (m_A)\boldsymbol{b} = (\boldsymbol{a}(\boldsymbol{x}))\boldsymbol{b}$
- *Bob*→*Alice*: $m_B= \boldsymbol{b}(\boldsymbol{x})$
- *Alice*: compute $S_A= (m_B)\boldsymbol{a} = (\boldsymbol{b}(\boldsymbol{x}))\boldsymbol{a}$

Common Secret

By Definition 1.1, $S_A = S_B$.

Remark. If the m_A, S_A , m_B, S_B are computed with some precision, then one has $S_A \approx S_B$ and additional exchange between Alice and Bob may be necessary.

Now we consider examples of commuting double actions coming from semigroups and their actions on sets.

Definition 1.2. A *semigroup* is a set A with an associative multiplication $A \times A \to A$, i.e.

$$(\boldsymbol{ab})\boldsymbol{c}=\boldsymbol{a}(\boldsymbol{bc})$$

for any $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ in A.

Example 1. Let X be a semigroup (i.e., a set with an associative multiplication) and let $A \subseteq X$ and $B \subseteq X$ be any subsets. Then the maps $A\times X \to X$, $X \times A \to X$ and $B \times X \to X$, $X \times B \to X$ given respectively by:

$$\boldsymbol{a}(\boldsymbol{x}) = (\boldsymbol{x})\boldsymbol{a} = \boldsymbol{a}\cdot\boldsymbol{x} \text{ and } \boldsymbol{b}(\boldsymbol{x}) = (\boldsymbol{x})\boldsymbol{b} = \boldsymbol{x}\cdot\boldsymbol{b}$$

constitute a commuting double action because $(\boldsymbol{a}(\boldsymbol{x}))\boldsymbol{b} = (\boldsymbol{a}\cdot\boldsymbol{x})\cdot\boldsymbol{b} = \boldsymbol{a}\cdot(\boldsymbol{x}\cdot\boldsymbol{b}) = (\boldsymbol{b}(\boldsymbol{x}))\boldsymbol{a}$.

Remark. A slightly more general example of two-sided multiplication in semigroups and groups was considered in ([8]).

Definition 1.3. Let M be a semigroup and let X be a set. A *left* action of M on X is a map $M \times X \to X$ (to be denoted by $(\boldsymbol{a}, \boldsymbol{x}) \to \boldsymbol{a}\cdot\boldsymbol{x}$ for any $\boldsymbol{a} \in A$, $\boldsymbol{x} \in X$) such that

(1.2) $$\boldsymbol{a}(\boldsymbol{bx}) = (\boldsymbol{a}\cdot\boldsymbol{b})\boldsymbol{x}$$

for any elements $\boldsymbol{a}$ and $\boldsymbol{b}$ of M and any $\boldsymbol{x} \in X$. A *right* action of a semigroup M on X is a map $M \times X \to X$ (to be denoted by $(\boldsymbol{x}, \boldsymbol{a}) \to \boldsymbol{xa}$ for any $\boldsymbol{a} \in M$, $\boldsymbol{x} \in X$) such that

(1.3) $$(\boldsymbol{xa})\boldsymbol{b} = \boldsymbol{x}(\boldsymbol{a}\cdot\boldsymbol{b})$$

for any elements $\boldsymbol{a}$ and $\boldsymbol{b}$ of M and any $\boldsymbol{x} \in X$.

Definition 1.4. Let M be a semigroup. Given two sets A and B and two pairs of maps φ_A, φ'_A: $A \to M$ and φ_B, φ'_B: $B \to M$, we say that the quadruple (φ_A, φ'_A, φ_B, φ'_B) *quasi-commutes* if

(1.4) $$\varphi'_B(\boldsymbol{b})\cdot\varphi_A(\boldsymbol{a}) = \varphi'_A(\boldsymbol{a})\cdot\varphi_B(\boldsymbol{b})$$

for all $\boldsymbol{a} \in A$ and $\boldsymbol{b} \in B$.

Lemma 1.5. Let M be a semigroup and let X, A, and B be sets. Fix a quasi-commuting quadruple of maps φ_A, φ'_A: $A \to M$ and φ_B, φ'_B: $B \to M$. Then:

(a) For any left action $M \times X \to X$ the following four maps $A \times X \to X$, $X \times A \to X$ and $B \times X \to X$, $X \times B \to X$ constitute a commuting double action of A and B on X:

(1.5) $$\boldsymbol{a}(\boldsymbol{x}) = \varphi_A(\boldsymbol{a})\boldsymbol{x},\ \boldsymbol{b}(\boldsymbol{x}) = \varphi_B(\boldsymbol{b})\boldsymbol{x},\ (\boldsymbol{x})\boldsymbol{a} = \varphi'_A(\boldsymbol{a})\boldsymbol{x},\ (\boldsymbol{x})\boldsymbol{b} = \varphi'_B(\boldsymbol{b})\boldsymbol{x}$$

for any $\boldsymbol{x} \in X$ and any $\boldsymbol{a} \in A$, $\boldsymbol{b} \in B$.

(b) For any right action $X \times M \to X$ the following four maps $A \times X \to X$, $X \times A \to X$ and $B \times X \to X$, $X \times B \to X$ constitute a commuting double action of A and B on X:

(1.6) $$\boldsymbol{a}(\boldsymbol{x}) = \boldsymbol{x}\varphi'_A(\boldsymbol{a}),\ \boldsymbol{b}(\boldsymbol{x}) = \boldsymbol{x}\varphi'_B(\boldsymbol{b}),\ (\boldsymbol{x})\boldsymbol{a} = \boldsymbol{x}\varphi_A(\boldsymbol{a}),\ (\boldsymbol{x})\boldsymbol{b} = \boldsymbol{x}\varphi_B(\boldsymbol{b})$$

for any $\boldsymbol{x} \in X$ and any $\boldsymbol{a} \in A$, $\boldsymbol{b} \in B$.

Proof. Prove (a). For any $\boldsymbol{x}\in X$ and any $\boldsymbol{a}\in A$, $\boldsymbol{b}\in B$ we have:

$$(\boldsymbol{a}(\boldsymbol{x}))\boldsymbol{b} = \varphi'_B(\boldsymbol{b})(\varphi_A(\boldsymbol{a})\boldsymbol{x}) = (\varphi'_B(\boldsymbol{b})\cdot\varphi_A(\boldsymbol{a}))\boldsymbol{x} = (\varphi'_A(\boldsymbol{a})\cdot\varphi_B(\boldsymbol{b}))\boldsymbol{x} = \varphi'_A(\boldsymbol{a})(\varphi_B(\boldsymbol{b}))\boldsymbol{x}) = (\boldsymbol{b}(\boldsymbol{x}))\boldsymbol{a} .$$

This proves (a). Prove (b) now.

$$(\boldsymbol{a}(\boldsymbol{x}))\boldsymbol{b} = (\boldsymbol{x}\varphi'_A(\boldsymbol{a}))\varphi_B(\boldsymbol{b}) = \boldsymbol{x}(\varphi'_A(\boldsymbol{a})\cdot\varphi_B(\boldsymbol{b})) = \boldsymbol{x}(\varphi'_B(\boldsymbol{b})\cdot\varphi_A(\boldsymbol{a})) = (\boldsymbol{x}\varphi'_B(\boldsymbol{b}))\varphi_A(\boldsymbol{a}) = (\boldsymbol{b}(\boldsymbol{x}))\boldsymbol{a} .$$

This proves the lemma. ■

Definition 1.6. Let M be a semigroup and let (α,α') and (β,β') be two pairs of elements of M. We say that these two pairs quasi-commute if

(1.7) $$\beta'\cdot\alpha=\alpha'\cdot\beta.$$

More generally, given two families $A=\{(\alpha_i,\alpha'_i), i=1,2,\dots, k\}$, $B=\{(\beta_j, \beta'_j), j=1,2,\dots, l\}$ of pairs of elements of M, we say that A and B *quasi-commute* if

(1.8) $$\beta'_j\cdot\alpha_i= \alpha'_i\cdot\beta_j$$

for all $i=1,2,\dots, k, j=1,2,\dots, l$.

The following example links Definitions 1.4 and 1.6 in the case when M is a ring.

Example 2. Let M be a ring and let $A=\{(\alpha_i, \alpha'_i) \mid i=1,2,\dots, k\}$, $B=\{(\beta_j, \beta'_j) \mid j=1,2,\dots, l\}$ be quasi-commuting families of pairs of elements in M. Define four maps $\varphi_A, \varphi'_A: \mathbb{Z}^k\to M$ and $\varphi_B, \varphi'_B: \mathbb{Z}^l\to M$ by the formula:

(1.9) $$\varphi_A(\boldsymbol{a})= \sum_{i=1}^{k} a_i\cdot\alpha_i , \quad \varphi'_A(\boldsymbol{a})=\sum_{i=1}^{k} a_i\cdot\alpha'_i , \quad \varphi_B(\boldsymbol{b})=\sum_{j=1}^{l} b_j\cdot\beta_j , \quad \varphi'_B(\boldsymbol{b})= \sum_{j=1}^{l} b_j\cdot\beta'_j$$

for any $\boldsymbol{a}=(a_1, a_2,\dots, a_k)\in \mathbb{Z}^k$, $\boldsymbol{b}=(b_1, b_2,\dots, b_l)\in \mathbb{Z}^l$.

Lemma 1.7. Let M be a ring and let $A=\{(\alpha_i, \alpha'_i) \mid i=1,2,\dots, k\}$, $B=\{(\beta_j, \beta'_j) \mid j=1,2,\dots, l\}$ be two quasi-commuting families of elements of M. Then the quadruple of maps φ_A, $\varphi'_A:\mathbb{Z}^k \to M$ and $\varphi_B,\varphi'_B:\mathbb{Z}^l \to M$ defined by (1.9) quasi-commutes (in the sense of Definition 1.4).

Proof. Define the map $\Psi: \mathbb{Z}^k\times\mathbb{Z}^l \to M$ by the formula

$$\Psi(\boldsymbol{a},\boldsymbol{b})= \varphi'_B(\boldsymbol{b}) \cdot\varphi_A(\boldsymbol{a}) - \varphi'_A(\boldsymbol{a}) \cdot\varphi_B(\boldsymbol{b})$$

for any $\boldsymbol{a} \in\mathbb{Z}^k$, $\boldsymbol{b}\in\mathbb{Z}^l$. In view of (1.4), our goal is to prove that $\Psi=0$. Indeed, Ψ is linear in $\boldsymbol{a}$ and linear in $\boldsymbol{b}$, that is:

$$\Psi(\boldsymbol{a},\boldsymbol{b})= \sum_{i=1}^{k} \sum_{j=1}^{l} a_i b_j\cdot\Psi(e_i, f_j) .$$

On the other hand, let $e_1, e_2, \dots, e_k$ be the basis for $\mathbb{Z}^k$ and $f_1, f_2, \dots, f_l$ be the standard basis for $\mathbb{Z}^l$. By definition, $\Psi(e_i, f_j) = \beta'_j\cdot\alpha_i- \alpha'_i\cdot\beta_j=0$ for all i and j by (1.7). Therefore, $\Psi=0$. ■

Remark. A key establishment scheme utilizing a particular case of Example 2 (in the case when all $\alpha_i, \alpha'_i, \beta_j, \beta'_j$ are certain powers of an element $S\in M$) was suggested in [7].

Example 3 (Diffie-Hellman). In the notation of Definition 1.4 let $M=A=B=\mathbb{Z}$, the set of all integers considered a semigroup under multiplication. Then raising elements of any group X into integer powers defines a commuting double action of M on X via:

$$\boldsymbol{a}(\boldsymbol{x})= (\boldsymbol{x})\boldsymbol{a}=\boldsymbol{x}^{\boldsymbol{a}}, \quad \boldsymbol{b}(\boldsymbol{x})=(\boldsymbol{x})\boldsymbol{b}=\boldsymbol{x}^{\boldsymbol{b}}$$

because $(\boldsymbol{x}^{\boldsymbol{a}})^{\boldsymbol{b}}=\boldsymbol{x}^{\boldsymbol{ab}}$.

In what follows we denote by $M_n(\mathbb{Z})$ the set of integer $n\times n$ matrices. This is a ring under matrix addition and matrix multiplication.

Our first main example below will generalize all examples of semigroup actions constructed in [7].

Main Example I.

- G is any group
- n is any natural number
- G^n denotes the n-th Cartesian power of G, i.e., the set of all n-tuples $\mathbf{g}=(g_1,\ldots,g_n)$ of elements of G
- $X_n=[G^n]\subseteq G^n$ is the set of all pairwise commuting tuples $\mathbf{g}=(g_1,\ldots,g_n)$, i.e.,

$$g_i\cdot g_j= g_j\cdot g_i$$

  for i, j=1,2,…, n
- Two families of quasi-commuting integer $n\times n$ matrices

$$A=\{(\alpha_i, \alpha'_i) \mid i=1,2,\ldots, k\},\ B=\{(\beta_j, \beta'_j) \mid j=1,2,\ldots, l\}$$

- A map (not action!) $G^n \times M_n(\mathbb{Z}) \to G^n$ is given by the formula: $(\mathbf{g},\boldsymbol{A}) \to \mathbf{g}^{\boldsymbol{A}}$ for any $\boldsymbol{A}=(a_{ij})\in M_n(\mathbb{Z})$, $\mathbf{g}=(g_1,\ldots,g_n)\in [G^n]$, where $\mathbf{g}^{\boldsymbol{A}}$ is the $\boldsymbol{A}$-th power of $\mathbf{g}$:

$$\mathbf{g}^{\boldsymbol{A}}=(g'_1,\ldots,g'_n),$$

  where

$$g'_j=\prod_{i=1}^{n} g_i^{a_{ij}} \tag{1.10}$$

Lemma 1.8. The assignment $(\mathbf{g},\boldsymbol{A}) \to \mathbf{g}^{\boldsymbol{A}}$ is a right action of $M_n(\mathbb{Z})$ on $X_n=[G^n]$:

$$X_n \times M_n(\mathbb{Z}) \to X_n, \tag{1.11}$$

i.e., for any $\boldsymbol{A}=(a_{ij})$, $\boldsymbol{B}=(b_{ij})\in M_n(\mathbb{Z})$ and any $\mathbf{g}\in X_n$ one has

$$(\mathbf{g}^{\boldsymbol{A}})^{\boldsymbol{B}}=\mathbf{g}^{\boldsymbol{AB}}. \tag{1.12}$$

Proof. It suffices to prove only (1.12). Indeed, using the fact that all g_i commute with each other, we have by (1.10) for all j:

$$((\mathbf{g}^{\boldsymbol{A}})^{\boldsymbol{B}})_j=\prod_{k=1}^{n}(\mathbf{g}^{\boldsymbol{A}})_k^{b_{kj}}=\prod_{k=1}^{n}\Big(\prod_{i=1}^{n} g_i^{a_{ij}}\Big)_k^{b_{kj}}=\prod_{i=1}^{n} g_i^{c_{ij}},$$

where

$$c_{ij}=\sum_{k=1}^{n} a_{ik}b_{kj}=(\boldsymbol{AB})_{ij}.$$

Therefore, $((\mathbf{g}^{\boldsymbol{A}})^{\boldsymbol{B}})_j=(\mathbf{g}^{\boldsymbol{AB}})_j$. This proves (1.12). The lemma is proved. ■

Below we propose our second main example of a commuting double action.

Main Example II.

- G is a group.
- m and n are natural numbers
- $M_{m\times n}(G)$ denotes the set of $m\times n$ matrices $\mathbf{g}=(g_{ij})$ with coefficients $g_{ij}\in G$
- $X_{m\times n}=[M_{m\times n}(G)]\subseteq M_{m\times n}(G)$ is the set of all those elements $\mathbf{g}=(g_{ij})\in M_{m\times n}(G)$ in which the entries pairwise commute, i.e.,

$$g_{ij}\cdot g_{kl}= g_{kl}\cdot g_{ij}$$

for all i, k=1, 2,…, m; j, l=1, 2,…, n

- Maps (not a com`muting double action!)

$$M_m(\mathbb{Z}) \times M_{m\times n}(G) \to M_{m\times n}(G),\ M_{m\times n}(G)\times M_m(\mathbb{Z})\to M_{m\times n}(G)$$
$$M_n(\mathbb{Z})\times M_{m\times n}(G) \to M_{m\times n}(G),\ M_{m\times n}(G)\times M_n(\mathbb{Z}) \to M_{m\times n}(G)$$

given by $(\mathbf{g})\boldsymbol{A}={}^{\boldsymbol{A}}\mathbf{g} = \boldsymbol{A}(\mathbf{g})$, $(\mathbf{g})\boldsymbol{B}= \mathbf{g}^{\boldsymbol{B}} =\boldsymbol{B}(\mathbf{g})$, where ${}^{\boldsymbol{A}}\mathbf{g}=(g'_{ij})$, $\mathbf{g}^{\boldsymbol{B}} =(g''_{ij})$ are given by the formula:

$$g'_{ij}=\prod_{k=1}^{m} g_{kj}^{a_{ik}}, \qquad g''_{ij}=\prod_{k=1}^{n} g_{ik}^{b_{kj}}$$

Lemma 1.9. These data define a commuting double action $M_m(\mathbb{Z})\times X_{m\times n} \to X_{m\times n}$ and $X_{m\times n}\times M_n(\mathbb{Z}) \to X$, i.e., $({}^{\boldsymbol{A}}\mathbf{g})^{\boldsymbol{B}}={}^{\boldsymbol{A}}(\mathbf{g}^{\boldsymbol{B}})$ for any $\boldsymbol{A}\in M_m(\mathbb{Z})$, $\boldsymbol{B}\in M_n(\mathbb{Z})$, $\mathbf{g}\in X_{m\times n}$.

Proof. It is equivalent to the associativity of the matrix multiplication:

$$(\boldsymbol{Ax})\boldsymbol{B}=\boldsymbol{A}(\boldsymbol{xB})$$

for any $m\times m$ matrix $\boldsymbol{A}$, any $m\times n$ matrix $\boldsymbol{x}$, and $n\times n$ matrix $\boldsymbol{B}$. ■

Section 2. Geometric Key Establishment I

In this section we present a key establishment scheme based on *Main Example I* and on the general right action key establishment scheme of Section 1. We will refer to it as geometric key establishment I (GKE I). First, we present the ideal GKE scheme (i.e., without any rounding).

Ideal Geometric Key Establishment I (GKE I) Scheme

Setup (non-secret parameters)

- n is a natural number
- $X_n=[0,1)^n$ is the semi-open n-dimensional cube, i.e., X_n is the n-th Cartesian power of the semi-open interval [0,1) of the real line. A point of X_n is an n-tuple $\mathbf{g}=(g_1, g_2,..., g_n)$, where each $g_i \in[0,1)$
- Two families of quasi-commuting integer $n\times n$ matrices

$$A=\{(\alpha_i, \alpha'_i) \mid i=1,2,\ldots, k\},\ B=\{(\beta_j, \beta'_j) \mid j=1,2,\ldots, l\}$$

- The right action $X_n\times M_n(\mathbb{Z})\to X_n$ is given by the formula

(2.1) $$(\mathbf{g},\boldsymbol{A}) \to \{\mathbf{g}\cdot\boldsymbol{A}\}$$

for any matrix $\boldsymbol{a}\in M_n(\mathbb{Z})$ and any $\mathbf{g}\in \mathbf{X}_n$, where for each vector $\boldsymbol{x}=(x_1, x_2,..., x_n)$ of real numbers we use the notation $\{\boldsymbol{x}\}=(\{x_1\}, \{x_2\},..., \{x_n\})$

Lemma 2.1. For any $\boldsymbol{a}=(a_1, a_2,\ldots, a_k)\in \mathbb{Z}^k$, $\boldsymbol{b}=(b_1, b_2,\ldots, b_l)\in \mathbb{Z}^l$, and $\mathbf{g}\in X_n$ one has

$$\{\{\mathbf{g}\cdot\varphi_A(\boldsymbol{a})\}\cdot\varphi'_B(\boldsymbol{b})\}=\{\mathbf{g}\cdot\varphi_A(\boldsymbol{a})\cdot\varphi'_B(\boldsymbol{b})\}=\{\mathbf{g}\cdot\varphi_B(\boldsymbol{b})\cdot\varphi'_A(\boldsymbol{a})\}=\{\{\mathbf{g}\cdot\varphi_B(\boldsymbol{b})\}\cdot\varphi'_A(\boldsymbol{a})\},$$

where $\varphi_A(\boldsymbol{a})$, $\varphi'_A(\boldsymbol{a})$, $\varphi_B(\boldsymbol{b})$, and $\varphi'_B(\boldsymbol{b})$ are defined in (1.9).

Proof. Taking the group G=[0,1) with the operation $\alpha*\beta=\{\alpha+\beta\}$ in Lemma 1.8 we obtain

$$\{\{\mathbf{g}\cdot \boldsymbol{A}\}\cdot \boldsymbol{B}\}=\{\mathbf{g}\cdot \boldsymbol{A}\cdot \boldsymbol{B}\}$$

for any $\mathbf{g}\in X_n$ and any $\boldsymbol{A}, \boldsymbol{B}\in M_n(\mathbb{Z})$.
This and the quasi-commutation equation (1.4) prove the lemma. ■

<u>*Protocol*</u>

- *Alice* and *Bob*: choose a non-secret $\mathbf{g}\in X_n$
- *Alice*: choose a secret $\boldsymbol{a}=(a_1, a_2,\ldots, a_k)\in \mathbb{Z}^k$
- *Bob*: choose a secret $\boldsymbol{b}=(b_1, b_2,\ldots, b_l)\in \mathbb{Z}^l$
- *Alice*→*Bob*: $m_A=\{\mathbf{g}\cdot\varphi_A(\boldsymbol{a})\}$
- *Bob*: compute $S_B=\{m_A\cdot\varphi'_B(\boldsymbol{b})\}=\{\{\mathbf{g}\cdot\varphi_A(\boldsymbol{a})\}\cdot\varphi'_B(\boldsymbol{b})\}$
- *Bob*→*Alice*: $m_B= \{\mathbf{g}\cdot\varphi_B(\boldsymbol{b})\}$
- *Alice*: compute $S_A= \{m_B\cdot\varphi'_A(\boldsymbol{a})\}=\{\{\mathbf{g}\cdot\varphi_B(\boldsymbol{b})\}\cdot\varphi'_A(\boldsymbol{a})\}$

<u>*Common Secret*</u>

By Lemma 2.1, $S_A = S_B$.

In order to present the *rounded* GKE I, we need the following notation.

Notation. For any real vectors $y = (y_1, y_2, \ldots, y_n)$, $z = (z_1, z_2, \ldots, z_n)$ the vector inequality $y\le z$ is equivalent to n scalar inequalities:

$$y_1\le z_1, y_2\le z_2, \ldots, y_n\le z_n.$$

Also the inequality $|y|<z$ means that $y<z$ and $-y<z$.

Denote by Round(z) the standard rounding of a real number z to the closest integer. Also for any real number $g\in[0,1)$ and any natural number P denote:

$$[g]_P=(\mathrm{Round}(gP))/P \text{ if } \mathrm{Round}(gP) < P,$$
$$[g]_P=0 \qquad \text{if } \mathrm{Round}(gP) = P.$$

For any natural n-tuple $\mathbf{P} = (P_1, P_2,..., P_n)$ and a real n-vector $\mathbf{g}=(g_1, g_2,..., g_n)$ such that each $g_i \in[0, 1)$, we define the **P**-rounding to a rational n-tuple $[\mathbf{g}]_\mathbf{P}$ by:

$$[\mathbf{g}]_\mathbf{P}=([g_1]_{P1},[g_2]_{P2},..., [g_n]_{Pn}).$$

For an n-tuple $\mathbf{P} = (P_1, P_2,..., P_n)$ of natural numbers denote $\mathbf{P}^*=(1/P_1,1/P_2,...,1/P_n)$.

Theorem 2.2. Let **P**, **Q**, and **K** be natural n-tuples. Then for any real n-vector **g** and any integer $n\times n$ matrices $\boldsymbol{A}=(a_{ij})$, $\boldsymbol{B}=(b_{ij})$, $\boldsymbol{A}'=(a'_{ij})$ and $\boldsymbol{B}'=(b'_{ij})$ satisfying $\boldsymbol{A}\cdot\boldsymbol{B}' = \boldsymbol{B}\cdot\boldsymbol{A}'$ and $\mathbf{Q}^*\cdot|\boldsymbol{A}'|\le \mathbf{K}^*$, $\mathbf{P}^*\cdot|\boldsymbol{B}'|\le \mathbf{K}^*$ one has: either at least one coordinate of $[\{[\{\mathbf{g}\cdot\boldsymbol{A}\}]_\mathbf{P}\cdot\boldsymbol{B}'\}]_\mathbf{K}$ equals 0, or at least one coordinate of $[\{[\{\mathbf{g}\cdot\boldsymbol{B}\}]_\mathbf{Q}\cdot\boldsymbol{A}'\}]_\mathbf{K}$ equals 0, or

$$|\{[\{\mathbf{g}\cdot\boldsymbol{A}\}]_\mathbf{P}\cdot\boldsymbol{B}'\}-\{[\{\mathbf{g}\cdot\boldsymbol{B}\}]_\mathbf{Q}\cdot\boldsymbol{A}'\}|< \mathbf{K}^*.$$

Therefore, $[\{[\{\mathbf{g}\cdot\boldsymbol{A}\}]_\mathbf{P}\}\cdot\boldsymbol{B}']_\mathbf{K} = [\{[\{\mathbf{g}\cdot\boldsymbol{A}\}]_\mathbf{Q}\}\cdot\boldsymbol{B}']_\mathbf{K} + \Delta$, where $\Delta = (\varepsilon_1/K_1, \varepsilon_2/K_2,\ldots, \varepsilon_n/K_n)$ and where each ε_i belongs to the set $\{-1, 0, 1\}$. In particular, the error vector Δ can take 3^n values.

For the proof of Theorem 2.2 see Appendix B.

Rounded GKE I Scheme

Setup (non-secret parameters):

- a natural number n
- natural n-tuples **P**,**Q**, and **K** as parameters of rounding
- mutually commuting subrings A and B of $M_n(\mathbb{Z})$

Protocol

- *Alice* and *Bob*: choose a non-secret $\mathbf{g} \in X_n$.
- *Alice*: choose a secret $\boldsymbol{a}=(a_1, a_2,\ldots, a_k)\in \mathbb{Z}^k$ such that $\mathbf{Q}^*\cdot|\varphi'_A(\boldsymbol{a})|\leq \mathbf{K}^*$
- *Bob*: choose a secret $\boldsymbol{b}=(b_1, b_2,\ldots, b_l)\in \mathbb{Z}^l$ such that $\mathbf{P}^*\cdot|\varphi'_B(\boldsymbol{b})|\leq \mathbf{K}^*$
- *Alice→Bob*: $m_A=[\{\mathbf{g}\cdot\varphi_A(\boldsymbol{a})\}]_\mathbf{P}$
- *Bob*: compute $S_B=[\{m_A\cdot\boldsymbol{b}\}]_\mathbf{K}=[\{[\{\mathbf{g}\cdot\varphi_A(\boldsymbol{a})\}]_\mathbf{P}\cdot\varphi'_B(\boldsymbol{b})\}]_\mathbf{K}$
- *Bob→Alice*: $m_B=[\{\mathbf{g}\cdot\varphi_B(\boldsymbol{b})\}]_\mathbf{Q}$
- *Alice*: compute $S_A=[\{m_B\cdot\varphi'_A(\boldsymbol{a})\}]_\mathbf{K}=[\{[\{\mathbf{g}\cdot\varphi_B(\boldsymbol{b})\}]_\mathbf{P}\cdot\varphi'_A(\boldsymbol{a})\}]_\mathbf{K}$

Common Secret

By Theorem 2.2, we have $S_A= S_B + (\varepsilon_1/K_1, \varepsilon_2/K_2,\ldots, \varepsilon_n/K_n)$, where each $\varepsilon_i \in\{-1, 0, 1\}$. In particular, the difference between S_A and S_B can take at most 3^n values. This difference can be eliminated in the follow-up communication of Alice and Bob. Thus, the shared secret is the vector S_A.

Remark. We express our gratitude to Gene Itkis for the idea to eliminate the difference between S_A and S_B using the follow-up communication of Alice and Bob.

Security of Rounded GKE I

Security of Rounded GKE I is based on hardness of the following is an analogue of the Discrete Logarithm Problem.

Given:

- a natural number n
- a subset $\boldsymbol{D}$ of $M_n(\mathbb{Z})$
- a natural n-tuple P and $\mathbf{g}\in X_n=[0, 1)^n$
- a vector $\boldsymbol{x}=[\{\mathbf{g}\cdot\boldsymbol{A}\}]_\mathbf{P}$ for some *unknown* $\boldsymbol{A}\in\boldsymbol{D}$

Compute: $\boldsymbol{A}'\in\boldsymbol{D}$ such that $\{\mathbf{g}\cdot\boldsymbol{A}'\}_\mathbf{P} = \boldsymbol{x}$

Clearly, the larger is the set $\boldsymbol{D}$ the harder is the problem. However, there is a natural limitation on the size of $\boldsymbol{D}$ because of the requirement of quasi-commutation of matrices $\boldsymbol{A}$ and $\boldsymbol{B}$. This and other GKE I – related problems will be analyzed in the work [4].

Numerical example. We take in the setup as above:

- $n=2$
- $\mathbf{P}=(10^{18}, 10^{18})$, $\mathbf{K}=(10^{10}, 10^{10})$ as the parameters of rounding
- $\mathbf{M}=(10^{8}, 10^{8})$.
- $A=B=\mathbb{Z}^2$ and for $\boldsymbol{a}=(a_0, a_1)\in \mathbb{Z}^2$ the 2×2 matrices $\varphi_A(\boldsymbol{a})$, $\varphi'_A(\boldsymbol{a})$, $\varphi_B(\boldsymbol{a})$, $\varphi'_B(\boldsymbol{a})$ are given by:

  $$\varphi_A(\boldsymbol{a})=\varphi'_A(\boldsymbol{a})=\varphi_B(\boldsymbol{a})=\varphi'_B(\boldsymbol{a})=\begin{bmatrix} a_0 & -a_1 \\ a_1 & a_0 \end{bmatrix}$$

  As defined, these matrices satisfy the quasi-commutation equation (1.4).

  Public *continuous* parameter: $\mathbf{g} = (g_1, g_2) =(\sqrt{2}, \sqrt{3})$.

Protocol. Alice chooses a pair of secret integers $(a_0, a_1) = (48176925, 18034725)$. Alice calculates the rounded vector

$$\mathbf{y}=(y_1, y_2)=([\{g_1a_0 + g_2a_1\}]_\mathbf{P}, [\{- g_1a_1+ g_2a_0 \}]_\mathbf{P}) .$$

That is,

$$\mathbf{y}=([\{\sqrt{2}\cdot 48176925+\sqrt{3}\cdot 18034725\}]_\mathbf{P}, [\{-\sqrt{2}\cdot 18034725+\sqrt{3}\cdot 48176925 \}]_\mathbf{P})=$$
$$([\{68132460.728431422183990297539596+31237060.000532620547511774721314\}]_\mathbf{P},$$
$$[\{-25504952.688669116604000035676723+83444881.852435233704474767836253\}]_\mathbf{P})$$
$$=(0.728964042731502072, 0.163766117100474732).$$

Each coordinate y_1, y_2 of this $\mathbf{y}$ has exactly 18 digits because $\mathbf{P}=(10^{18}, 10^{18})$. Alice sends this rounded vector $\mathbf{y}$ to Bob. Independently Bob chooses a pair of secret integers $(b_0, b_1) = (19082792, 27045821)$. Bob calculates the vector

$$\mathbf{z}=(z_1, z_2)=([\{g_1b_0 + g_2b_1\}]_\mathbf{P}, [\{- g_1b_1+ g_2b_0 \}]_\mathbf{P})$$

That is,

$$\mathbf{z}= ([\{ \sqrt{2}\cdot 19082792 + \sqrt{3}\cdot 27045821\}]_\mathbf{P}, [\{-\sqrt{2}\cdot 27045821+ \sqrt{3}\cdot 19082792\}]_\mathbf{P}) =$$
$$([\{26987143.254344799212512475172839 + 46844736.104413300451707772339473\}]_\mathbf{P},$$
$$[\{-38248566.863715063905876737732694 + 33052365.294268911065907204826118\}]_\mathbf{P})$$
$$= (0.358758099664220248, 0.430553847160030467)$$

and sends this vector $\mathbf{z}$ to Alice.

Upon receiving the vector $\mathbf{y}$ from Alice, Bob calculates the rounded vector $\mathbf{k}=(k_1, k_2)$ by the formula:

$$\mathbf{k} =(k_1, k_2) = ([\{ y_1b_0 + y_2b_1\}]_\mathbf{K}, [\{- y_1b_1+ y_2b_0 \}]_\mathbf{K}) .$$

That is,

$$\mathbf{k}=([\{0.728964042731502072\cdot 19082792+0.163766117100474732\cdot 27045821\}]_\mathbf{K},$$
$$[\{-0.728964042731502072\cdot 27045821+ 0.163766117100474732\cdot 19082792\}]_\mathbf{K})=$$
$$=([\{13910669.202924365887545024+4429189.088964478616694972\}]_\mathbf{K},$$
$$[\{-19715431.015152556100441112+3125114.749276002412011744\}]_\mathbf{K})$$
$$=(0.2918888445, 0.7341234463)$$

Each coordinate k_1, k_2 of this $\mathbf{k}$ has exactly 10 digits because $\mathbf{K}=(10^{10}, 10^{10})$.

Upon receiving the vector $\mathbf{z}$ from Bob, Alice calculates the rounded vector $\mathbf{k}'=(k'_1,k'_2)$ by the formula:

$$\mathbf{k}'=(k'_1, k'_2)=([\{z_1\cdot a_0 + z_2\cdot a_1\}]_\mathbf{K}, [\{- z_1\cdot a_1+ z_2\cdot a_0 \}]_\mathbf{K}) .$$

That is,

$$\mathbf{k}' =([\{ 0.358758099664220248\cdot 48176925 + 0.430553847160030467\cdot 18034725\}]_{\mathbf{K}},$$
$$[\{- 0.358758099664220248\cdot 18034725+ 0.430553847160030467\cdot 48176925\}]_{\mathbf{K}})$$
$$=([\{17283862.0606656640713774+ 7764920.231223180463966575\}]_{\mathbf{K}},$$
$$[\{- 6470103.6689668045121118 + 20742760.403090250806373975\}]_{\mathbf{K}})$$
$$=(0.2918888445, 0.7341234463)$$

Thus, the vector (0.2918888445, 0.7341234463) is the secret shared by Alice and Bob.

Remark. Unlike in the general case of GKE, in this example Alice and Bob did not need any follow-up communication in order to establish the common secret out of **k** and **k'**. They know that **k**=**k'** because, on the one hand, Theorem 2.2 guarantees each coordinate of the difference **k**-**k'** can be either 0 or $\pm 10^{-10}$ and, on the other hand, for each coordinate of each vector **k** and **k'** the 10^{th} digit is neither 0 nor 9.

Section 3. Geometric Key Establishment II

In this section we present a key establishment scheme based on Main Example II and on the general commuting double action key establishment scheme of Section 1. We will refer to it as geometric key establishment II (GKE II).

First, we present the ideal GKE II scheme (i.e., without any rounding).

Ideal Geometric Key Establishment II (GKE II) Scheme

Setup (public parameters):

- m and n are natural numbers
- $X_{m\times n}=M_{m\times n}([0,1))$ is the set of all $m\times n$ matrices with coefficients in the semi-open interval [0,1). Each point of $X_{m\times n}$ is an $m\times n$ matrix $\mathbf{g}=(g_{ij})$, where each $g_{ij} \in[0,1)$

For each real $m\times n$ matrix $x=(x_{ij})$ we use the notation $\{x\}=(\{x_{ij}\})$, where $\{x_{ij}\}$ stands for the fractional part of the real number x_{ij}.

Lemma 3.1. For any integer matrices $\boldsymbol{A}\in M_m(\mathbb{Z})$, $\boldsymbol{B}\in M_n(\mathbb{Z})$, and any $\mathbf{g}\in X_{m\times n}$ one has

(3.1) $$\{\{\boldsymbol{A}\cdot\mathbf{g}\}\cdot\boldsymbol{B}\}=\{\boldsymbol{A}\cdot\mathbf{g}\cdot\boldsymbol{B}\}=\{\boldsymbol{A}\cdot\{\mathbf{g}\cdot\boldsymbol{B}\}\} .$$

Proof. We will reduce the statement to Lemma 1.9. It suffices to show (similarly to the proof of Lemma 2.1) that the set G=[0,1) is a group. Indeed, we have already shown that in the proof of Lemma 2.1.This proves the lemma. ■

Protocol

- *Alice* and *Bob*: choose a non-secret $\mathbf{g}\in X_{m\times n}$
- *Alice*: choose a secret $\boldsymbol{A}\in M_m(\mathbb{Z})$
- *Bob*: choose a secret $\boldsymbol{B}\in M_n(\mathbb{Z})$
- *Alice→Bob*: $m_A=\{\boldsymbol{A}\cdot\mathbf{g}\}$
- *Bob*: compute $S_B=\{m_A\cdot\boldsymbol{B}\}=\{\{\boldsymbol{A}\cdot\mathbf{g}\}\cdot\boldsymbol{B}\}$
- *Bob→Alice*: $m_B= \{\mathbf{g}\cdot\boldsymbol{B}\}$
- *Alice*: compute $S_A=\{\boldsymbol{A}\cdot m_B\}=\{ \boldsymbol{A}\cdot\{\mathbf{g}\cdot\boldsymbol{B}\}\}$

Common Secret

By Lemma 3.1, $S_A = S_B$.

In order to present the *rounded* GKE II, we need the following notation.

Notation. For any real $m\times n$ matrices $y = (y_{ij})$ and $z = (y_{ij})$, the matrix inequality $y \le z$ is equivalent to $m\times n$ scalar inequalities: $y_{ij}\le z_{ij}$ for i=1,2,…,m; j=1,2,…,n. Also the inequality $|y|<z$ means that $y<z$ and $-y<z$.

For a natural $m\times n$ matrix $\mathbf{P} = (P_{ij})$ and a real $m\times n$ matrix $\mathbf{g} = (g_{ij})$ such that each $g_{ij}\in[0,1)$, define the **P**-rounding to a rational $m\times n$ matrix $[\mathbf{g}]_\mathbf{P}\in X_{m\times n}$ by the formula:
$[\mathbf{g}]_\mathbf{P}=([g_{ij}]_{P_{ij}})$,
where $[g]_P$ is the same as in Rounded GKE I. For any natural $m\times n$ matrix $\mathbf{P} = (P_{ij})$ we denote $\mathbf{P}^*= (1/P_{ij})$.

Theorem 3.2. Let be **P**, **Q**, and **K** be natural $m\times n$ matrices. Then for any integer $m\times m$ matrix $\boldsymbol{A}$ and any integer $n\times n$ matrix $\boldsymbol{B}$ such that $|\boldsymbol{A}|\cdot\mathbf{Q}^*\le \mathbf{K}^*$, $\mathbf{P}^*\cdot|\boldsymbol{B}|\le \mathbf{K}^*$ one has: either at least one coefficient of the matrix $[\{[\{\boldsymbol{A}\cdot\mathbf{g}\}]_\mathbf{P}\cdot\boldsymbol{B}\}]_\mathbf{K}$ equals 0, or at least one coefficient of the matrix $[\{\boldsymbol{A}\cdot[\{\mathbf{g}\cdot\boldsymbol{B}\}]_\mathbf{Q}\}]_\mathbf{K}$ equals 0, or $|\{[\{\boldsymbol{A}\cdot\mathbf{g}\}]_\mathbf{P}\cdot\boldsymbol{B}\}-\{\boldsymbol{A}\cdot[\{\mathbf{g}\cdot\boldsymbol{B}\}]_\mathbf{Q}\}|<\mathbf{K}^*$.
Therefore, $[\{[\{\boldsymbol{A}\cdot\mathbf{g}\}]_\mathbf{P}\cdot\boldsymbol{B}\}]_\mathbf{K} = [\{\boldsymbol{A}\cdot[\{\mathbf{g}\cdot\boldsymbol{B}\}]_\mathbf{Q}\}]_\mathbf{K}+\Delta$, where $\Delta = (\varepsilon_{ij}/K_{ij})$ and where each ε_{ij} belongs to the set $\{-1, 0, 1\}$. In particular, the error matrix Δ can take 3^{mn} values.

For the proof of Theorem 3.2 see Appendix B**.**

Rounded GKE II Scheme

Setup (public parameters):

- natural numbers m and n
- natural $m\times n$ matrices **P**, **Q**, and **K** as parameters of rounding

Protocol

- *Alice* and *Bob*: choose a non-secret $\mathbf{g}\in X_{m\times n}$
- *Alice*: choose a secret $\boldsymbol{A}\in M_m(\mathbb{Z})$ such that $|\boldsymbol{A}|\cdot\mathbf{Q}^*\le \mathbf{K}^*$
- *Bob*: choose a secret $\boldsymbol{B}\in M_n(\mathbb{Z})$ such that $\mathbf{P}^*\cdot|\boldsymbol{B}|\le \mathbf{K}^*$
- *Alice→Bob*: $m_A=[\{\boldsymbol{A}\cdot\mathbf{g}\}]_\mathbf{P}$
- *Bob*: compute $S_B=[\{m_A\cdot\boldsymbol{B}\}]_\mathbf{K}=[\{[\{\boldsymbol{A}\cdot\mathbf{g}\}]_\mathbf{P}\cdot\boldsymbol{B}\}]_\mathbf{K}$
- *Bob→Alice*: $m_B=[\{\mathbf{g}\cdot\boldsymbol{B}\}]_\mathbf{Q}$
- *Alice*: compute $S_A=[\{\boldsymbol{A}\cdot m_B\}]_\mathbf{K}=[\{[\boldsymbol{A}\cdot\{\mathbf{g}\cdot\boldsymbol{B}\}]_\mathbf{P}\}]_\mathbf{K}$

Common Secret

By Theorem 3.2, one has $S_A= S_B + (\varepsilon_{ij}/K_{ij})$, where each $\varepsilon_{ij} \in\{-1, 0, 1\}$. In particular, the difference between A_A and S_B can take at most $3^{m\cdot n}$ values. This difference can be eliminated in the follow-up communication of Alice and Bob. Thus, the shared secret is the vector S_A.

The problem of security of Rounded GKE II follows the discussed above pattern of Rounded GKE I and will also be analyzed in [4].

Numerical example. We take in the setup as above:

- $m=n=2$
- $\mathbf{P}=(P_{ij})$, where each $P_{ij}=10^9$, $\mathbf{K}=(K_{ij})$ where each $K_{ij}=10^5$
- $\mathbf{M}=(M_{ij})$, where each $M_{ij}=10^3$

Public *continuous* parameter:

$$\mathbf{g} = (g_{ij}) = \begin{bmatrix} \sqrt{2} & \sqrt{3} \\ \sqrt{5} & \sqrt{7} \end{bmatrix}$$

Protocol. Suppose that Alice chooses a secret integer 2×2 matrix $\boldsymbol{A}$:

$$\boldsymbol{A} = \begin{bmatrix} 123 & 456 \\ 817 & 391 \end{bmatrix}$$

Alice calculates the 2×2 matrix $\mathbf{y}=[\{\boldsymbol{A}\cdot\mathbf{g}\}]$ each element of which rounded to 9 decimal places:

$$\mathbf{y}=[\{\boldsymbol{A}\cdot\mathbf{g}\}] = \begin{bmatrix} 0.595265912 & 0.504847176 \\ 0.715059661 & 0.574272410 \end{bmatrix}$$

and sends this 2×2 matrix $\mathbf{y}$ to Bob. Suppose that at independently Bob chooses a secret integer 2×2 matrix $\boldsymbol{B}$:

$$\boldsymbol{B} = \begin{bmatrix} 691 & 378 \\ 529 & 109 \end{bmatrix}$$

Bob calculates the 2×2 matrix $\mathbf{z} =[\{\mathbf{g}\cdot\boldsymbol{B}\}]$ each element of which rounded to 9 decimal places:

$$\mathbf{z} = [\{\mathbf{g}\cdot\boldsymbol{B}\}]= \begin{bmatrix} 0.476448804 & 0.366264602 \\ 0.725416006 & 0.620588401 \end{bmatrix}$$

and sends this 2×2 matrix $\mathbf{z}$ to Alice. Upon receiving the 2×2 matrix $\mathbf{y}$ from Alice, Bob calculates the 2×2 matrix $\mathbf{k}=[\{\mathbf{y}\cdot\boldsymbol{B}\}]$ with the precision 5 decimal places after dot:

$$\mathbf{k} = [\{\mathbf{y}\cdot\boldsymbol{B}\}] = \begin{bmatrix} 0.39290 & 0.03885 \\ 0.89633 & 0.88824 \end{bmatrix}$$

Upon receiving the 2×2 matrix $\mathbf{z}$ from Bob, Alice calculates the 2×2 matrix $\mathbf{k}'=[\{\boldsymbol{A}\cdot\mathbf{z}\}]$ with the precision 5 decimal places after dot:

$$\mathbf{k}' = [\{\boldsymbol{A}\cdot\mathbf{z}\}] = \begin{bmatrix} 0.39290 & 0.03885 \\ 0.89633 & 0.88824 \end{bmatrix}$$

Remark. Unlike in the general case of GKE II, in this example Alice and Bob did not need any follow-up communication in order to establish the common secret out of **k** and **k**'. They know that **k**=**k**' because, on the one hand, Theorem 3.2 guarantees that each matrix coefficient of the difference **k**-**k**' can be either 0 or $\pm 10^{-5}$ and, on the other hand, for each coefficient of each matrix **k** and **k**' the 5^{th} digit is neither 0 nor 9.

Appendix A. General Key Establishment Scheme and its rounded versions

We start with a natural generalization of Diffie-Hellman protocol. Apparently, this generalization is well known, but we have failed to find references. Hence, we will take liberty to call it 'basic key establishment scheme.'

Definition A.1. Let A, B and X, Y_A, Y_B, Z be sets. Let $A\times X\to Y_A$, $B\times Y_A\to Z$, and $B\times X\to Y_B$, $A\times Y_B \to Z$ be a quadruple of maps (we denote them respectively by $(\boldsymbol{a}, \boldsymbol{x}) \to \boldsymbol{a}(\boldsymbol{x})$, $(\boldsymbol{b}, \boldsymbol{y}) \to \boldsymbol{b}(\boldsymbol{y})$, and $(\boldsymbol{b}, \boldsymbol{x}) \to \boldsymbol{b}(\boldsymbol{x})$, $(\boldsymbol{a}, \boldsymbol{y}') \to \boldsymbol{a}(\boldsymbol{y}')$ for any elements $\boldsymbol{a}\in A$, $\boldsymbol{b} \in B$, $\boldsymbol{x}\in X$, $\boldsymbol{y}\in Y_A$, $\boldsymbol{y}'\in Y_B$). We say that the quadruple is *commuting* if:

(A.1) $$\boldsymbol{a}(\boldsymbol{b}(\boldsymbol{x})) = \boldsymbol{b}(\boldsymbol{a}(\boldsymbol{x}))$$

for any $\boldsymbol{a}\in A$, $\boldsymbol{b}\in B$, $\boldsymbol{x}\in X$.

The basic key establishment scheme consists of the following setup and protocol.

Basic key establishment scheme

Setup:

- sets A and B (of private parameters)
- a set X (of shared parameters)
- a set Y_A (of Alice's transmittable elements)
- a set Y_B (of Bob's transmittable elements)
- a set Z (of shared secret elements)
- a commuting quadruple of maps $A\times X\to Y_A$, $B\times Y_A\to Z$, $B\times X\to Y_B$, $A\times Y_B \to Z$

Protocol

- *Alice* and *Bob*: choose a non-secret $\boldsymbol{x}\in X$
- *Alice*: choose a secret element $\boldsymbol{a}\in A$
- *Bob*: choose a secret element $\boldsymbol{b}\in B$
- *Alice*→*Bob*: $m_A=\boldsymbol{a}(\boldsymbol{x})$
- *Bob*: compute $S_B= \boldsymbol{b}(m_A) = \boldsymbol{b}(\boldsymbol{a}(\boldsymbol{x}))$
- *Bob*→*Alice*: $m_B= \boldsymbol{b}(\boldsymbol{x})$
- *Alice*: compute $S_A= \boldsymbol{a}(m_B) = \boldsymbol{a}(\boldsymbol{b}(\boldsymbol{x}))$

<u>*Common Secret*</u>

By Definition A.1, $S_A = S_B$.

Remark. The scheme is secure if the following problem is hard: given $\boldsymbol{x} \in X$ and $\boldsymbol{y} \in Y_A$, find $\boldsymbol{a} \in A$ such that $\boldsymbol{y} = \boldsymbol{a}(\boldsymbol{x})$. In the case of the original Diffie-Hellman scheme ([5]), this problem is known as the *discrete logarithm problem*.

Of course, for the purpose of implementation of this basic scheme, it is natural to require that all the involved sets A, B, X, Y_A, Y_B, and Z are finite. In Sections 2 and 3 we presented a method for generation of a large family of finite key establishment schemes each of which represents a non-trivial approximation of the basic scheme. The richness of the family stems from its origin in an *infinite* or even *continuous* instantiation of the basic scheme.

Generalizing rounded schemes introduced in Sections 2 and 3, we propose here a general *rounded key establishment* (RKE) scheme. In the following definitions and results we need a mathematical concept of 'metric space'. For the standard references, see e.g. [6].

Definition A.2. A *metric space* is a pair (X, d), where X is a set and $d: X \times X \to \mathbb{R}_{\geq 0}$ is a *distance function* on X satisfying:

- (symmetry) $d(\boldsymbol{x}, \boldsymbol{x}') = d(\boldsymbol{x}', \boldsymbol{x})$ for all $\boldsymbol{x}, \boldsymbol{x}' \in X$
- $d(\boldsymbol{x}, \boldsymbol{x}') = 0$ if and only if $\boldsymbol{x} = \boldsymbol{x}'$
- (triangle inequality) $d(\boldsymbol{x}, \boldsymbol{x}'') \geq d(\boldsymbol{x}, \boldsymbol{x}') + d(\boldsymbol{x}', \boldsymbol{x}'')$ for all $\boldsymbol{x}, \boldsymbol{x}', \boldsymbol{x}'' \in X$

Definition A.3. Let (X, d) and (Y, d) be metric spaces. Then a map $F: X \to Y$ is called *metric* if there exists a positive constant C such that $d(F(\boldsymbol{x}), F(\boldsymbol{x}')) \leq C \cdot d(\boldsymbol{x}, \boldsymbol{x}')$ for any $\boldsymbol{x}, \boldsymbol{x}' \in X$. More generally, given a function $f: A \to \mathbb{R}_{>0}$, we say that a map $A \times X \to Y$ (which we denote $(\boldsymbol{a}, \boldsymbol{x}) \to \boldsymbol{a}(\boldsymbol{x})$) is *f-Lipschitz* if $d(\boldsymbol{a}(\boldsymbol{x}), \boldsymbol{a}(\boldsymbol{x}')) \leq f(\boldsymbol{a}) \cdot d(\boldsymbol{x}, \boldsymbol{x}')$ for any $\boldsymbol{x}, \boldsymbol{x}' \in X$, $\boldsymbol{a} \in A$.

Definition A.4. Let (X, d) be a metric space. Let K be a discrete subset of X. Consider a map $[\cdot]: X \to K$ (to be denoted by $\boldsymbol{x} \to [\boldsymbol{x}]$) such that for each $\boldsymbol{x} \in X$ the distance from $\boldsymbol{x}$ to $[\boldsymbol{x}]$ does not exceed the distance from $\boldsymbol{x}$ to any other point of K. We refer to any such map as K-*rounding* on (X, d).

In what follows we will consider only infinite or even uncountable metric spaces.

Definition A.5. Let (X, d) be a metric space. Let us consider an infinite ascending chain $X_1 \subset X_2 \subset X_3 \subset \ldots \subset X_k \subset \ldots$ of discrete subsets (each inclusion is strict), and let $\mathbf{r} = \{r_k\}$, $k = 1, 2, \ldots$ be a decreasing sequence of positive real numbers converging to 0. Given an infinite family $[\cdot]_k: X \to X_k$ of X_k-roundings on (X, d) for $k = 1, 2, \ldots$, we say that the family $[\cdot]_k$ is $\mathbf{r}$-*saturated* if $d(\boldsymbol{x}, [\boldsymbol{x}]_k) \leq r_k$ for any point $\boldsymbol{x}$ and for each natural number k.

Definition A.6. Let (X, d) be a metric space, $\boldsymbol{x}$ be a point of X, and r be a positive real number. Denote by $B(\boldsymbol{x}; r)$ the set of all points $\boldsymbol{x}' \in X$ such that $d(\boldsymbol{x}, \boldsymbol{x}') < r$. We refer to $B(\boldsymbol{x}; r)$ as the *open ball* of radius r centered at $\boldsymbol{x}$.

Definition A.7. Let (X, d) be a metric space, $\mathbf{r}=\{r_k\}$ be a sequence of positive real numbers, and N be a natural number. We say that an ascending chain $X_1\subset X_2\subset X_3\subset \ldots\subset X_k\subset\ldots$ of subsets of X is **(r**, N**)**-*uniform* if

$$|B(\boldsymbol{x};r_k)\cap X_k|<N$$

for every $\boldsymbol{x}\in X_k$ and each k=1,2,… .

Informally speaking, (**r**,N)-uniform chains in X provide good approximations of points of X similarly to the way in which rational numbers provide good approximations of real numbers.

Definition A.8. For a given (**r**, N)-uniform ascending chain $X_1\subset X_2\subset X_3\subset \ldots\subset X_k\subset \ldots$ in a metric space (X, d) we say that two points $\boldsymbol{k}$ and $\boldsymbol{k}'$ of X_k are *neighbors* if $d(\boldsymbol{k}, \boldsymbol{k}')<r_k$.

By definition, any point $\boldsymbol{k}\in X_k$ has at most N neighbors.

Theorem A.9. Let A, B, and X be sets, and $A\times X \to Y_A$, $B\times X\to Y_B$ be maps. Let (Y_A, d), (Y_B, d), and (Z, d) be metric spaces, and let $B\times Y_A \to Z$ be a g-Lipschitz map, $A\times Y_B \to Z$ be a g'-Lipschitz map. Also let $[\cdot]_m: Y_A \to (Y_A)_m$ be an **r**-saturated rounding on (Y_A, d), $[\cdot]'_m:Y_B \to (Y_B)_m$ be an **r′**-saturated family of roundings on (Y_B, d), and $[\cdot]''_k:Z \to (Z)_k$ be an **r″**-saturated family of roundings on (Y_B, d) such that the ascending chain $Z_1\subset Z_2\subset Z_3\subset \ldots\subset Z_k\subset\ldots$ is (3**r″,** N)-*uniform*. Then for any commuting elements $\boldsymbol{a}\in A$ and $\boldsymbol{b}\in B$ such that $g(\boldsymbol{b})<r''_k/(2r_m)$, $g'(\boldsymbol{a})<r''_k/(2r'_m)$ (for some natural m, k) and any $\boldsymbol{x}\in X$ one has:

$[\boldsymbol{a}([\boldsymbol{b}(\boldsymbol{x})]'_m)]''_k$ and $[\boldsymbol{b}([\boldsymbol{a}(\boldsymbol{x})]_m)]''_k$ are neighbors.

Proof. By definition of saturated families of roundings, one has for any m:

$$d(\boldsymbol{a}(\boldsymbol{x}),[\boldsymbol{a}(\boldsymbol{x})]_m)\le r_m,\ d(\boldsymbol{b}(\boldsymbol{x}),[\boldsymbol{b}(\boldsymbol{x})]'_m)\le r'_m\ .$$

Therefore, for given m and k we have:

$$d(\boldsymbol{b}(\boldsymbol{a}(\boldsymbol{x})), \boldsymbol{b}([\boldsymbol{a}(\boldsymbol{x})]_m))\le g(\boldsymbol{b})\cdot d(\boldsymbol{a}(\boldsymbol{x})), [\boldsymbol{a}(\boldsymbol{x})]_m) \le g(\boldsymbol{b})\cdot r_m < r''_k /2,$$

$$d(\boldsymbol{a}(\boldsymbol{b}(\boldsymbol{x})), \boldsymbol{a}([\boldsymbol{b}(\boldsymbol{x})]'_m))\le g'(\boldsymbol{a})\cdot d(\boldsymbol{b}(\boldsymbol{x})), [\boldsymbol{a}(\boldsymbol{x})]'_m) \le g'(\boldsymbol{a})\cdot r'_m < r''_k /2\ .$$

Denote $\boldsymbol{z}=(\boldsymbol{a}(\boldsymbol{b}(\boldsymbol{x}))=(\boldsymbol{b}(\boldsymbol{a}(\boldsymbol{x}))$. Then $d(\boldsymbol{z}, \boldsymbol{b}([\boldsymbol{a}(\boldsymbol{x})]_m))\le r''_k /2$, $d(\boldsymbol{z}, \boldsymbol{a}([\boldsymbol{b}(\boldsymbol{x})]_m))\le r''_k /2$.

Denote $\boldsymbol{k}_1=[\boldsymbol{a}([\boldsymbol{b}(\boldsymbol{x})]'_m)]''_k$ and $\boldsymbol{k}_2=[\boldsymbol{b}([\boldsymbol{a}(\boldsymbol{x})]_m)]''_k$. Note that

$$d(\boldsymbol{k}_1, \boldsymbol{a}([\boldsymbol{b}(\boldsymbol{x})]'_m))\le r''_k,\ d(\boldsymbol{k}_2, \boldsymbol{b}([\boldsymbol{a}(\boldsymbol{x})]_m))\le r''_k\ .$$

Then, by the triangle inequality,

$$d(\boldsymbol{z}, \boldsymbol{k}_1) \le d(\boldsymbol{z}, \boldsymbol{a}([\boldsymbol{b}(\boldsymbol{x})]_m))+d(\boldsymbol{k}_1, \boldsymbol{a}([\boldsymbol{b}(\boldsymbol{x})]_m)) < r''_k/2 + r''_k =3r''_k/2\ ,$$

$$d(\boldsymbol{z}, \boldsymbol{k}_2) \le d(\boldsymbol{z}, \boldsymbol{a}([\boldsymbol{b}(\boldsymbol{x})]_m))+d(\boldsymbol{k}_2, \boldsymbol{b}([\boldsymbol{a}(\boldsymbol{x})]_m)) < r''_k/2 + r_k =3r''_k/2\ .$$

Finally, again by the triangle inequality,

$$d(\boldsymbol{k}_1, \boldsymbol{k}_2) \le d(\boldsymbol{z}, \boldsymbol{k}_1)+d(\boldsymbol{z}, \boldsymbol{k}_2) <3r''_k/2+3r''_k/2=3r''_k$$

That is, $\boldsymbol{k}_1$ and $\boldsymbol{k}_2$ are neighbors. Theorem A.9 is proved. ■

Based on this general result we propose the following general *rounded* key establishment scheme.

<u>Rounded key establishment (RKE) scheme</u>:

Setup

- sets A and B of private parameters
- a set X of shared parameters
- infinite metric spaces (Y_A, d) and (Y_B, d) of transmittable elements
- an infinite metric space (Z, d) of shared secret elements
- maps $A\times X\to Y_A$, $B\times X\to Y_B$, a g-Lipschitz map $B\times Y_A\to Z$, and a g'-Lipschitz map $A\times Y_B\to Z$ such that the quadruple of these maps is commuting
- an $\mathbf{r}$-saturated family of roundings $[\cdot]_m$: $Y_A\to(Y_A)_m$ on (Y_A, d) and an $\mathbf{r'}$-saturated family of roundings $[\cdot]'_m$: $Y_B\to(Y_B)_m$ on (Y_B, d)
- an $\mathbf{r''}$-saturated family of roundings $[\cdot]''_k$: $Z\to(Z)_k$ on (Z, d) such that the ascending chain $Z_1\subset Z_2\subset Z_3\subset \ldots\subset Z_k\subset\ldots$ is $(3\mathbf{r''},\mathrm{N})$-*uniform*

Protocol

- *Alice* and *Bob*: choose a shared parameter $\boldsymbol{x}\in X$ and natural numbers m, k
- *Alice*: choose a private $\boldsymbol{a}\in A$ such that $g'(\boldsymbol{a})< r''_k/(2r'_m)$
- *Bob*: choose a private $\boldsymbol{b}\in B$ such that $g(\boldsymbol{b})<r''_k/(2r_m)$
- *Alice→Bob*: $m_A=[\boldsymbol{a}(\boldsymbol{x})]_m$
- *Bob*: compute $S_B= [\boldsymbol{b}(m_A)]''_k= [\boldsymbol{b}([\boldsymbol{a}(\boldsymbol{x})]_m)]''_k$
- *Bob→Alice*: $m_B= [\boldsymbol{b}(\boldsymbol{x})]'_m$
- *Alice*: compute $S_A= [\boldsymbol{a}(m_B)]''_k = [\boldsymbol{a}([\boldsymbol{b}(\boldsymbol{x})]'_m)]''_k$

<u>Common Secret</u>

By Theorem A.9, S_A and S_B are neighbors. Therefore, after making at most N choices, and without revealing the elements they computed, Alice and Bob select S_A as their shared secret.

Appendix B. Proof of results of Sections 2 and 3

Proof of Theorem 2.2. By definition, one has:

$$[\{\mathbf{g}\cdot\boldsymbol{A}\}]_{\mathbf{P}}=\{\mathbf{g}\cdot\boldsymbol{A}\} + \theta_1,\ \{\mathbf{g}\cdot\boldsymbol{B}\}_{\mathbf{Q}} = \{\mathbf{g}\cdot\boldsymbol{B}\} + \theta_2,$$

where $-\frac{1}{2}\cdot\mathbf{P}^{-1}\le \theta_1\le \frac{1}{2}\cdot\mathbf{P}^{-1}$ and $-\frac{1}{2}\cdot\mathbf{Q}^{-1}\le \theta_2\le \frac{1}{2}\cdot\mathbf{Q}^{-1}$. Therefore,

$$[\{\mathbf{g}\cdot\boldsymbol{A}\}]_{\mathbf{P}}\cdot\boldsymbol{B'} = (\{\mathbf{g}\cdot\boldsymbol{A}\}+\theta_1)\cdot\boldsymbol{B'}=\{\mathbf{g}\cdot\boldsymbol{A}\}\cdot\boldsymbol{B'} +\theta_1\cdot\boldsymbol{B'}= \{\mathbf{g}\cdot\boldsymbol{A}\}\cdot\boldsymbol{B'} + \mathbf{E}_1,$$

where $\mathbf{E}_1=\theta_1\cdot\boldsymbol{B'}$. Similarly,

$$[\{\mathbf{g}\cdot\boldsymbol{B}\}]_{\mathbf{Q}}\cdot\boldsymbol{A'} = (\{\mathbf{g}\cdot\boldsymbol{B}\}+\theta_2)\cdot\boldsymbol{A'}=\{\mathbf{g}\cdot\boldsymbol{B}\}\cdot\boldsymbol{A'} +\theta_2\cdot\boldsymbol{A'}= \{\mathbf{g}\cdot\boldsymbol{B}\}\cdot\boldsymbol{A'} +\mathbf{E}_2\ ,$$

where $\mathbf{E}_2=\theta_2\cdot\boldsymbol{A'}$.

By the assumptions, one has:

$$|\mathbf{E}_1| = |\theta_1\cdot\boldsymbol{B'}| \le \tfrac{1}{2}\cdot|\boldsymbol{P}^{-1}\cdot\boldsymbol{B'}|< \tfrac{1}{2}\cdot\boldsymbol{P}^{-1}\cdot\boldsymbol{B'} \le \tfrac{1}{2}\cdot\boldsymbol{K}^{-1},\ |\mathbf{E}_2| = |\theta_2\cdot\boldsymbol{A'}| \le \tfrac{1}{2}\cdot|\boldsymbol{Q}^{-1}\cdot\boldsymbol{A'}| < \tfrac{1}{2}\cdot\boldsymbol{Q}^{-1}\cdot\boldsymbol{B'} \le \tfrac{1}{2}\cdot\boldsymbol{K}^{-1}.$$

In its turn, the inequality $|\mathbf{E}_1|\leq 1/2\cdot \boldsymbol{K}^{-1}$ implies that either the vector $\{\{\mathbf{g}\cdot \boldsymbol{A}\}_{\boldsymbol{P}}\cdot \boldsymbol{B}'\}_{\boldsymbol{K}}$ has a coordinate equal to 0 or:

$$\{[\{\mathbf{g}\cdot \boldsymbol{A}\}]_{\mathbf{P}}\cdot \boldsymbol{B}'\}= \{\{\mathbf{g}\cdot \boldsymbol{A}\}\cdot \boldsymbol{B}' + \mathbf{E}_1\}= \{\{\mathbf{g}\cdot \boldsymbol{A}\}\cdot \boldsymbol{B}'\} + \mathbf{E}_1=\{\mathbf{g}\cdot \boldsymbol{A}\cdot \boldsymbol{B}'\} + \mathbf{E}_1 .$$

Similarly, the inequality $|\mathbf{E}_2|\leq 1/2\cdot \boldsymbol{K}^{-1}$ implies that either the vector $\{\{\mathbf{g}\cdot \boldsymbol{B}\}_{\boldsymbol{Q}}\cdot \boldsymbol{A}'\}_{\boldsymbol{K}}$ has a coordinate equal to 0 or:

$$\{[\{\mathbf{g}\cdot \boldsymbol{B}\}]_{\mathbf{Q}}\cdot \boldsymbol{A}'\}= \{\{\mathbf{g}\cdot \boldsymbol{B}\}\cdot \boldsymbol{A}' + \mathbf{E}_2\}= \{\{\mathbf{g}\cdot \boldsymbol{B}\}\cdot \boldsymbol{A}'\} + \mathbf{E}_2=\{\mathbf{g}\cdot \boldsymbol{B}\cdot \boldsymbol{A}'\} + \mathbf{E}_2 .$$

Since $\boldsymbol{A}\cdot \boldsymbol{B}'= \boldsymbol{B}\cdot \boldsymbol{A}'$, one has $\{[\{\mathbf{g}\cdot \boldsymbol{A}\}]_{\mathbf{P}}\cdot \boldsymbol{B}'\}-\{[\{\mathbf{g}\cdot \boldsymbol{B}\}]_{\mathbf{Q}}\cdot \boldsymbol{A}'\}= \mathbf{E}_1- \mathbf{E}_2$. Finally note that

$$|\mathbf{E}_1- \mathbf{E}_2| \leq |\mathbf{E}_1| + |\mathbf{E}_2| < 1/2\cdot \mathbf{K}^{-1} +1/2\cdot \mathbf{K}^{-1} = \mathbf{K}^{-1}$$

Theorem 2.2 is proved. ■

Proof of Theorem 3.2. By definition, one has $[\{\boldsymbol{A}\cdot \mathbf{g}\}]_{\mathbf{P}} = \{\boldsymbol{A}\cdot \mathbf{g}\}+\theta_1$, $[\{\mathbf{g}\cdot \boldsymbol{B}\}]_{\mathbf{Q}}=\{\mathbf{g}\cdot \boldsymbol{B}\}+\theta_2$, where θ_1 and θ_2 are real $m\times n$ matrices such that

$$-½\ \mathbf{P}^*\leq \theta_1\leq ½\ \mathbf{P}^* \text{ and } -½\ \mathbf{Q}^*\leq \theta_2\leq ½\ \mathbf{Q}^*.$$

Therefore, $([\{\boldsymbol{A}\cdot \mathbf{g}\}]_{\mathbf{P}})\cdot \boldsymbol{B}=(\{\boldsymbol{A}\cdot \mathbf{g}\} + \theta_1)\cdot \boldsymbol{B}=\{\boldsymbol{A}\cdot \mathbf{g}\}\cdot \boldsymbol{B} + \theta_1\cdot \boldsymbol{B}= \{\boldsymbol{A}\cdot \mathbf{g}\}\cdot \boldsymbol{B}+\mathbf{E}_1$, where $\mathbf{E}_1=\theta_1\cdot \boldsymbol{B}$. Similarly, $\boldsymbol{A}\cdot([\{\mathbf{g}\cdot \boldsymbol{B}\}]_{\mathbf{Q}})=\boldsymbol{A}\cdot(\{\mathbf{g}\cdot \boldsymbol{B}\}+\theta_2\cdot \mathbf{Q}^{-1})= \boldsymbol{A}\cdot\{\mathbf{g}\cdot \boldsymbol{B}\}+\boldsymbol{A}\cdot\theta_2= \boldsymbol{A}\cdot\{\mathbf{g}\cdot \boldsymbol{B}\}+\mathbf{E}_2$,where $\mathbf{E}_2= \boldsymbol{A}\cdot\theta_2$. By the assumptions, one has:

$$|\mathbf{E}_1| = |\theta_1\cdot \boldsymbol{B}| \leq ½\cdot|\mathbf{P}^*\cdot \boldsymbol{B}| < ½\cdot\mathbf{K}^*,\ |\mathbf{E}_2| = |\boldsymbol{A}\cdot\theta_2| \leq ½\cdot|\boldsymbol{A}\cdot\mathbf{Q}^*| < ½\cdot\mathbf{K}^*.$$

In its turn, this implies that either at least one coefficient of the matrix $[\{[\{\boldsymbol{A}\cdot \mathbf{g}\}]_{\mathbf{P}}\cdot \boldsymbol{B}\}]_{\mathbf{K}}$ equals 0, or at least one coefficient of the matrix $[\{\boldsymbol{A}\cdot[\{\mathbf{g}\cdot \boldsymbol{B}\}]_{\mathbf{Q}}\}]_{\mathbf{K}}$ equals 0, or:

$$\{([\{\boldsymbol{A}\cdot \mathbf{g}\}]_{\mathbf{P}})\cdot \boldsymbol{B}\}= \{\{\boldsymbol{A}\cdot \mathbf{g}\}\cdot \boldsymbol{B}+\mathbf{E}_1\}= \{\{\boldsymbol{A}\cdot \mathbf{g}\}\cdot \boldsymbol{B}\}+\mathbf{E}_1=\{\boldsymbol{A}\cdot \mathbf{g}\cdot \boldsymbol{B}\}+\mathbf{E}_1 .$$

Similarly, the above implies that either at least one coefficient of the matrix $[\{\boldsymbol{A}\cdot[\{\mathbf{g}\cdot \boldsymbol{B}\}]_{\mathbf{Q}}\}]_{\mathbf{K}}$ is 0 or:

$$\{\boldsymbol{A}\cdot([\{\mathbf{g}\cdot \boldsymbol{B}\}]_{\mathbf{Q}})\}= \{\boldsymbol{A}\cdot\{\mathbf{g}\cdot \boldsymbol{B}\}+\mathbf{E}_2\}=\{\boldsymbol{A}\cdot\{\mathbf{g}\cdot \boldsymbol{B}\}\}+\mathbf{E}_2=\{\boldsymbol{A}\cdot \mathbf{g}\cdot \boldsymbol{B}\}+\mathbf{E}_2 .$$

Therefore

$$\{([\{\boldsymbol{A}\cdot \mathbf{g}\}]_{\mathbf{P}})\cdot \boldsymbol{B}\}-\{\boldsymbol{A}\cdot([\{\mathbf{g}\cdot \boldsymbol{B}\}]_{\mathbf{Q}})\}= \mathbf{E}_1 - \mathbf{E}_2 .$$

Finally note that

$$|\mathbf{E}_1- \mathbf{E}_2| \leq |\mathbf{E}_1| + |\mathbf{E}_2| < 1/2\cdot\mathbf{K}^* + 1/2\cdot \mathbf{K}^* = \mathbf{K}^*.$$

Theorem 3.2 is proved. ■

References

1. I. Anshel, M. Anshel, and D. Goldfeld, "An algebraic method for public-key cryptography," *Mathematical Research Letters* **6**, (1999). 1-5.
2. I. Anshel, M. Anshel, and D. Goldfeld, A Linear Time Matrix Key Agreement Protocol, preprint, http://www.ipam.ucla.edu/publications/cry2002/cry2002_dgoldfeld.pdf
3. I. Anshel, M. Anshel, and D. Goldfeld, "Non-abelian key agreement protocols," Discrete Appl. Math. 130 (2003), no. 1, 3-12.
4. A. Berenstein, L. Chernyak, G. Itkis, ArKE: "Arithmetic Key Establishment System and its Security," in preparation.
5. W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transaction on Information Theory vol. IT 22 (November 1976), pp. 644-654.
6. A. Kolmogorov, and S. Fomin, *Introductory real analysis*. Dover Publications, Inc., New York, 1975.
7. G. Maze, C. Monico, and J. Rosenthal. "A public key cryptosystem based on actions by semigroups." In Proceedings of the 2002 IEEE International Symposium on Information Theory, page 266, Lausanne, Switzerland, 2002.
8. V.M. Sidel'nikov, M.A. Cherepnev, V.V. Yashchenko, Systems of open distribution of keys on the basis of noncommutative semigroups, Russian Acad. Sci. Dokl. Math., vol. 48 (1994), No. 2, 384-386.

---

[i] Department of Mathematics, University of Oregon, Eugene, Oregon.
[ii] Institute for Self-Organizing Systems, LLC. Boston, Massachusetts.