Geometric Key Establishment

9/12/2004

Arkady Berenstein[1] and Leon Chernyak[2]

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 ([3]), 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 – two-sided 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 the action of braid semigroups on the braid groups ([1]), and an action of the semigroup of integer $n\times n$ matrices on finite commutative groups ([5]).

Although two-sided actions are well-known in mathematics, we are unaware of application of this concept in cryptography. In the present work we construct an algebra-geometric key establishment (AGKE) scheme which is based primarily on the concept of two-sided action.

Typically, Diffie-Hellman-like schemes involve time-consuming exponentiation procedures in finite fields or finite groups. Unlike this, GKE and AGKE do not use any exponentiation. We bypassed exponentiation by replacing the semigroup actions on finite groups with actions (or two-sided 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, therefore, uses only multiplication of real numbers by integers and addition of real numbers in its key creation.

[1] Affiliation: University of Oregon, Department of Mathematics.
[2] Affiliation: Institute of Genometric Systems, Inc.

First computer implementations of the cube-based scheme work with a much higher speed than all known implementations of Diffie-Hellman. Preliminary estimations show that GKE and AGKE are resistant to basic attacks. This resistance follows the pattern of the discrete logarithm problem. A more detailed study of GKE and AGKE security is a work [2] 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, the 3-dimensional sphere, 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 or AGKE in a real device, we, based on the ordinary rounding of real numbers, developed 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 such a rich family of discretizations for GKE and AGKE, 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 and AGKE, our concept of RKE will bring new interesting examples of key establishment schemes.

The paper is organized as follows:

In *Section* 1 we overview key establishment paradigms based on semigroup actions. Then we introduce a key establishment scheme based on two-sided action. We also introduced very general examples of semigroup actions and two-sided actions. In the following sections of the present work these examples provide the basis for our GKE and AGKE schemes

Section 2 is devoted to introduction and study of our first main example – Geometric Key Establishment (GKE). We start with a description of an ideal GKE 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 protocols work.

Section 3 is devoted to introduction and study of our second main example – Algebro-Geometric Key Establishment (AGKE). The section is structured similarly to Section 2.

We start with a description of an ideal AGKE 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 AGKE protocols work.

In *Appendix A* of this paper, 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-theoretical 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 our 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.

Section 1. Key establishment schemes based on semigroup actions

In this section we introduce a class of key establishment schemes which we refer to as *metric* key establishment (MKE) schemes. This class of schemes is based on the mathematical concept of *metric action* of a semigroup on a *metric space*.

We start with the standard mathematical definitions leading to the concept of the metric actions of semigroups. Then we will formulate a theorem that each metric action brings about an infinite family of discrete approximate actions. We conclude the section with the schemes of metric key establishment which are based on this family of discrete approximate actions.

Definition 1.1. 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.

Definition 1.2. Let A be a semigroup and let X be a set. A *left* action of A on X is a map $A\times X \to X$ (to be denoted by $(\boldsymbol{a}, \boldsymbol{x}) \to \boldsymbol{a}(\boldsymbol{x})$ for any $\boldsymbol{a} \in A, \boldsymbol{x} \in X$) such that

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

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

A *right* action of A on X is a map A×X → X (to be denoted by $(\boldsymbol{x},\boldsymbol{a}) \to (\boldsymbol{x})\boldsymbol{a}$ for any $\boldsymbol{a}\in$A, $\boldsymbol{x} \in$ X) such that

$$((\boldsymbol{x})\boldsymbol{a})\boldsymbol{b} = (\boldsymbol{x})(\boldsymbol{ab}) \tag{1.2}$$

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

Lemma 1.3. Let A be a semigroup, X be a set, and let A×X → X be a left action. Then

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

for any $\boldsymbol{x}\in$X and any $\boldsymbol{a}$, $\boldsymbol{b} \in$ A such that $\boldsymbol{ab} = \boldsymbol{ba}$. Similarly, if X×A → X is a right action, then

$$((\boldsymbol{x})\boldsymbol{a})\boldsymbol{b} = ((\boldsymbol{x})\boldsymbol{b})\boldsymbol{a} \tag{1.4}$$

for any $\boldsymbol{x}\in$X and any $\boldsymbol{a}$, $\boldsymbol{b} \in$ A such that $\boldsymbol{ab} = \boldsymbol{ba}$.

Proof. For any $\boldsymbol{a}$, $\boldsymbol{b} \in$ A such that $\boldsymbol{ab} = \boldsymbol{ba}$ and for any $\boldsymbol{x}\in$X we have:

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

Similarly,

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

This proves the lemma. ■

The result of Lemma 1.3 is widely used in key establishment protocols. The following classical example illustrates the typical usage of this result.

Let X be a group and let A= $\mathbb{Z}$ be the set of all integers considered a semigroup under multiplication. Then the setting $\boldsymbol{a}(\boldsymbol{x}) = \boldsymbol{x}^{\boldsymbol{a}}$ defines a left action of A on X (which action consists of raising elements of X into integer powers). Clearly, this action is simultaneously a right action because A= $\mathbb{Z}$ is a commutative semigroup. Obviously, the formula (1.3) holds for any integers $\boldsymbol{a}$ and $\boldsymbol{b}$ and any element $\boldsymbol{x}\in$ X.

We propose the following generalization of this classical example, which also generalizes examples of semigroup actions constructed in [5].

Main Example 1. Let G be any group and n be any natural number. Denote by G^n 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. Now let $X=[G^n] \subseteq G^n$ be the set of all pairwise commuting tuples $\mathbf{g}=(g_1,\ldots,g_n)$, i.e.,

$$g_k g_m = g_m g_k$$

for all $m, k\in\{1,2,\ldots,n\}$.

Note that if G is a commutative group or if n=1, then $[G^n] = G^n$ (for an arbitrary non-commutative group G the sub-space $[G^n]$ can have a very complicated structure).

Let $A_n=\mathrm{Mat}_n(\mathbb{Z})$, which is the set of all integer $n\times n$ matrices. Clearly, A_n is a semigroup under the matrix multiplication. Define a map $[G^n] \times A_n \to G^n$ by the formula:

$$(\mathbf{g})\boldsymbol{a} = \mathbf{g}^{\boldsymbol{a}}$$

for any $\boldsymbol{a}=(a_{ij})\in A_n$, $\mathbf{g}=(g_1,\ldots,g_n)\in [G^n]$, where $\mathbf{g}^{\boldsymbol{a}}$ is the $\boldsymbol{a}$-th power of $\mathbf{g}$:

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

where

$$g'_j=\prod_{i=1}^{n} g_i^{a_{ij}} \tag{1.5}$$

Clearly, for each matrix $\boldsymbol{a}\in A_n$ and any element $\mathbf{g}=(g_1,\ldots,g_n)\in[G^n]$ the power $\mathbf{g}^{\boldsymbol{a}}$ also belongs to $[G^n]$. Therefore, the assignment $(\mathbf{g},\boldsymbol{a})\rightarrow (\mathbf{g})\boldsymbol{a}=\mathbf{g}^{\boldsymbol{a}}$ defines a map

$$[G^n]\times A_n \rightarrow [G^n]. \tag{1.6}$$

Lemma 1.4. The map $[G^n]\times A_n \rightarrow [G^n]$ given by (1.6) is a right action of the semigroup $A_n=\mathrm{Mat}_n(\mathbb{Z})$ on the set $X=[G^n]$. That is, for any integer $n\times n$ matrices $\boldsymbol{a}=(a_{ij})$, $\boldsymbol{b}=(b_{ij})$, and any commuting n-tuple $\mathbf{g}=(g_1,\ldots,g_n)\in[G^n]$ one has

$$(\mathbf{g}^{\boldsymbol{a}})^{\boldsymbol{b}}=\mathbf{g}^{\boldsymbol{ab}}. \tag{1.7}$$

Proof. It suffices to prove only (1.7). Indeed, using the fact that all g_i^{a} commute with all g_j^{b}, we have by (1.5) for all j:

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

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 (1.7).

The lemma is proved. ■

We will construct below even more general class of actions in which the semigroup property is not required.

Definition 1.5. Let A,B, and X be sets. A pair of maps $A\times X\rightarrow X$ and $X\times B\rightarrow X$ (which we denote respectively as: $(\boldsymbol{a},\boldsymbol{x})\rightarrow \boldsymbol{a}(\boldsymbol{x})$ and $(\boldsymbol{x},\boldsymbol{b})\rightarrow (\boldsymbol{x})\boldsymbol{b}$) is a *two-sided action* if:

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

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

The simplest example of a two-sided action is as follows.

Lemma 1.6. Let X be a semigroup and let $A\subseteq X$ be a sub-semigroup (i.e., A is a subset of X closed under the multiplication $A\times A \rightarrow A$). And let B be another sub-semigroup of X. Then the maps $A\times X\rightarrow X$ and $X\times B\rightarrow X$ given respectively by:

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

constitute a two-sided action.

Proof. We have:

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

due to the associativity of the multiplication in the semigroup X. ■

Below we propose our main example of a two-sided action.

Main Example 2. Let G be a group. Denote by $\mathrm{Mat}_{m\times n}(G)$ the set of $m\times n$ matrices $\mathbf{g}=(g_{ij})$ with coefficients $g_{ij}\in G$. Now let $[\mathrm{Mat}_{m\times n}(G)]\subseteq \mathrm{Mat}_{m\times n}(G)$ be the set of all those elements $\mathbf{g}=(g_{ij})\in \mathrm{Mat}_{m\times n}(G)$ in which the entries pairwise commute, that is,

$$g_{ij}g_{kl}=g_{kl}g_{ij}$$

for all $i,k=1,2,\ldots,m$, $j,l=1,2,\ldots,n$.

Note that if G is a commutative group, then $[\mathrm{Mat}_{m\times n}(G)]=\mathrm{Mat}_{m\times n}(G)$.

For each $m\times m$ matrix $\boldsymbol{a}=(a_{ij})$ with integer coefficients, and any $\mathbf{g}=(g_{ij})\in [\mathrm{Mat}_{m\times n}(G)]$ define the *left* $\boldsymbol{a}$-th power ${}^{\boldsymbol{a}}\mathbf{g}$ by the formula

$${}^{\boldsymbol{a}}\mathbf{g}=(g'_{ij}),$$

where

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

By definition, for each matrix $\boldsymbol{a}$ the assignment $\mathbf{g}\to {}^{\boldsymbol{a}}\mathbf{g}$ defines a transformation $[\mathrm{Mat}_{m\times n}(G)]\to [\mathrm{Mat}_{m\times n}(G)]$.

Also for each $n\times n$ matrix $\boldsymbol{b}=(b_{ij})$ and any $\mathbf{g}=(g_{ij})\in [\mathrm{Mat}_{m\times n}(G)]$ define $\mathbf{g}^{\boldsymbol{b}}$ to be the *right* $\boldsymbol{b}$-th power of $\mathbf{g}$:

$$\mathbf{g}^{\boldsymbol{b}}=(g'_{ij}),$$

where

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

By definition, for each matrix $\boldsymbol{b}$ the assignment $\mathbf{g}\to \mathbf{g}^{\boldsymbol{b}}$ defines a transformation $[\mathrm{Mat}_{m\times n}(G)]\to [\mathrm{Mat}_{m\times n}(G)]$.

Lemma 1.7. In the notation as above the maps $A_m\times[\mathrm{Mat}_{m\times n}(G)]\to[\mathrm{Mat}_{m\times n}(G)]$ and $[\mathrm{Mat}_{m\times n}(G)]\times A_n\to[\mathrm{Mat}_{m\times n}(G)]$ given respectively by:

$$(\boldsymbol{a},\mathbf{g})\to {}^{\boldsymbol{a}}\mathbf{g} \text{ and } (\mathbf{g},\boldsymbol{b})\to \mathbf{g}^{\boldsymbol{b}}$$

constitute a two-sided action, that is,

$$({}^{\boldsymbol{a}}\mathbf{g})^{\boldsymbol{b}}={}^{\boldsymbol{a}}(\mathbf{g}^{\boldsymbol{b}}).$$

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

$$\boldsymbol{(ax)b=a(xb)}$$

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

That is, the operations of raising to the left and right powers commute (so we denote the resulting $(\boldsymbol{a}, \boldsymbol{b})$-th power by ${}^{\boldsymbol{a}}\mathbf{g}^{\boldsymbol{b}}$).

A general semigroup key establishment scheme was suggested in [5] (in particular, a class of key establishment schemes has been constructed in [5] based on A_n-action on G^n in the case when the group G is finite and commutative). For reader's convenience we present here this general scheme.

Left action key establishment scheme

Setup

- a semigroup A
- a set X
- a left semigroup action $A \times X \rightarrow X$

Protocol

1. Two communicating parties (let us call them Alice and Bob) choose $\boldsymbol{x} \in X$.
2. Alice chooses a secret element $\boldsymbol{a} \in A$ and Bob independently chooses a secret element $\boldsymbol{b} \in A$ in such a way that $\boldsymbol{ab} = \boldsymbol{ba}$.
3. Alice computes $\boldsymbol{a}(\boldsymbol{x})$ and sends it to Bob via an open channel and Bob computes $\boldsymbol{b}(\boldsymbol{x})$ and sends it to Alice via an open channel.
4. Alice computes the secret element $\boldsymbol{k}_1=\boldsymbol{a}(\boldsymbol{b}(\boldsymbol{x}))$ by applying $\boldsymbol{a}$ to the received element $\boldsymbol{b}(\boldsymbol{x})$; and Bob computes the secret element $\boldsymbol{k}_2=\boldsymbol{b}(\boldsymbol{a}(\boldsymbol{x}))$ by applying $\boldsymbol{b}$ to the received element $\boldsymbol{a}(\boldsymbol{x})$.

The elements $\mathbf{k}_1$ and $\mathbf{k}_2$ equal by *Lemma 1.1* (and they also equal $(\boldsymbol{ba})(\boldsymbol{x})=(\boldsymbol{ab})(\boldsymbol{x})$) and therefore constitute secret key shared by Alice and Bob.

Remark. Choosing the commuting elements $\boldsymbol{a}$ and $\boldsymbol{b}$ by Alice and Bob independently is not a trivial task. However, there is a way to guarantee a solution for the task in the case when A is a *ring*. Alice and Bob may construct commuting elements $\boldsymbol{a}$ and $\boldsymbol{b}$ as follows. They start with a (public) shared element $S \in A$, and then:

1. Alice chooses an n-tuple of secret integers $(a_1, a_2,\ldots,a_n)$, and Bob independently chooses an m-tuple of secret integers $(b_1, b_2,\ldots,b_m)$.
2. Alice computes the (secret) element $\boldsymbol{a}=a_1S+a_2S^2+\ldots+a_nS^n$ and Bob independently computes the (secret) matrix $\boldsymbol{b}=b_1S+b_2S^2+\ldots+b_mS^m$ (hence $\boldsymbol{ab} = \boldsymbol{ba}$).

Replacing the left action by a right action in the above scheme we obtain the *right action key establishment scheme*. This right action key establishment scheme along with the above method of obtaining commuting elements will be used in Section 2 – in the ideal GKE scheme and its rounded version.

The following key establishment scheme is based on the proposed above concept of a two-sided action. The advantage of the scheme is that the scheme bypasses the problem of choosing commuting elements $\boldsymbol{a}$ and $\boldsymbol{b}$ (of a given semigroups).

Two-sided action key establishment scheme

Setup

- Sets A, B, and X.
- a two-sided action $A\times X \rightarrow X$ and $X\times B \rightarrow X$

Protocol

1. Two communicating parties (let us call them Alice and Bob) choose $\boldsymbol{x}\in X$.
2. Alice chooses a secret element $\boldsymbol{a}\in A$ and Bob independently chooses a secret element $\boldsymbol{b}\in B$.
3. Alice computes $\boldsymbol{a}(\boldsymbol{x})$ and sends it to Bob via an open channel and Bob computes $(\boldsymbol{x})\boldsymbol{b}$ and sends it to Alice via an open channel.
4. Alice computes the secret element $\boldsymbol{k}_1=\boldsymbol{a}((\boldsymbol{x})\boldsymbol{b})$ by applying $\boldsymbol{a}$ to the received element $(\boldsymbol{x})\boldsymbol{b}$; and Bob computes the secret element $\boldsymbol{k}_2=(\boldsymbol{a}(\boldsymbol{x}))\boldsymbol{b}$ by applying $\boldsymbol{b}$ to the received element $\boldsymbol{a}(\boldsymbol{x})$.

By Definition 1.5 of two-sided actions the elements $\mathbf{k}_1$ and $\mathbf{k}_2$ equal and therefore constitute secret key shared by Alice and Bob.

Section 2. Geometric Key Establishment

In this section we present a key establishment scheme based on our first main example and the general right action key establishment scheme of Section 1. We will refer to it as geometric key establishment (GKE).

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

Ideal Geometric Key Establishment (GKE) Scheme

Setup

- n is a natural number (it is the dimension of the scheme).
- $A_n=\mathrm{Mat}_n(\mathbb{Z})$ is the semigroup of all integer matrices under the multiplication.
- $X_n=[0,1)^n$ is the semi-open n-dimensional cube, X is the n-th Cartesian power of the semi-open interval [0,1) of the real line. Each point of X_n is an n-tuple

$$\mathbf{g}=(g_1, g_2,..., g_n)\ ,$$

  where each $g_i \in [0,1)$.

- The map $[0,1)^n \times A_n \rightarrow [0,1)^n$ is given by the formula

(2.1) $$(\mathbf{g})\boldsymbol{a} = \{\mathbf{g}\cdot\boldsymbol{a}\}$$

for any matrix $\boldsymbol{a}\in A_n$ and any $\mathbf{g}\in[0,1)^n$, where for each vector $\boldsymbol{x}=(x_1, x_2,..., x_n)$ of real numbers we use the notation

(2.2) $$\{\boldsymbol{x}\}=(\{x_1\}, \{x_2\},..., \{x_n\}),$$

where $\{x_i\}$ stands for the fractional part of the real number x_i.

The following fact is a corollary of *Lemma 1.4*.

Lemma 2.1. The map $[0,1)^n \times A_n \to [0,1)^n$ given by (2.1) is a right action of the semigroup $A_n=\mathrm{Mat}_n(\mathbb{Z})$ on the set $X_n=[0,1)^n$. That is, for any integer $n\times n$ matrices $\boldsymbol{a}=(a_{ij})$, $\boldsymbol{b}=(b_{ij})$, and any n-tuple $\mathbf{g}=(g_1,\ldots,g_n)\in[0,1)^n$ one has

(2.3) $$\{\{\mathbf{g}\cdot\boldsymbol{a}\}\cdot\boldsymbol{b}\}=\{\mathbf{g}\cdot\boldsymbol{a}\cdot\boldsymbol{b}\}$$

Proof. In order to reduce the statement to *Lemma 1.4* it suffices to show that the set G=[0,1) with the following operation:

$$\alpha*\beta=\{\alpha+\beta\}$$

is a group. Indeed, the operation is associative, it has the unit 0, and the inverse of each $\alpha\in[0,1)$ is $\{-\alpha\}$.

This proves the lemma. ■

Protocol

1. Two communicating parties (let us call them Alice and Bob) choose a non-secret n-tuple $\mathbf{g}$ in $X=[0,1)^n$ and a matrix S in $A_n=\mathrm{Mat}_n(\mathbb{Z})$.
2. Alice chooses an n-tuple of secret integers $(a_0,\ldots,a_{n-1})$, and Bob independently chooses an n-tuple of secret integers $(b_0,\ldots,b_{n-1})$.
3. Alice computes the (secret) matrix $\boldsymbol{a}= a_0\cdot I+a_1\cdot S+a_2\cdot S^2+\ldots+ a_{n-1}\cdot S^{n-1}$ and Bob independently computes the (secret) matrix $\boldsymbol{b}= b_0\cdot I+b_1\cdot S+b_2\cdot S^2+\ldots+ b_{n-1}\cdot S^{n-1}$, where I is the identity matrix (so that one guarantees the commutation $\boldsymbol{a}\cdot\boldsymbol{b} = \boldsymbol{b}\cdot\boldsymbol{a}$).
4. Alice computes the tuple $\{\mathbf{g}\cdot\boldsymbol{a}\}$ and sends it to Bob via an open channel and Bob computes the tuple $\{\mathbf{g}\cdot\boldsymbol{b}\}$ and sends it to Alice via an open channel.
5. Alice computes the tuple $\boldsymbol{k}_1=\{\{\mathbf{g}\cdot\boldsymbol{b}\}\cdot\boldsymbol{a}\}$; and Bob computes the tuple $\boldsymbol{k}_2=\{\{\mathbf{g}\cdot\boldsymbol{a}\}\cdot\boldsymbol{b}\}$.

The tuples $\boldsymbol{k}_1$and $\boldsymbol{k}_2$ are equal and therefore constitute the secret shared by Alice and Bob. The equality of the tuples follows from the formula (2.3).

Now we present our main example – *rounded* GKE. Below we will use the following notation.

For any real vector $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ and $\boldsymbol{z} = (z_1, z_2, \ldots, z_n)$, the vector inequality $\boldsymbol{y} \le \boldsymbol{z}$ 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

$$|\boldsymbol{y}|<\boldsymbol{z}$$

means that $\boldsymbol{y}<\boldsymbol{z}$ and $-\boldsymbol{y}<\boldsymbol{z}$.

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:

$$[g]_P=(\text{Round}(gP))/P$$

if Round(gP) < P, and

$$[g]_P=0$$

if Round(gP) = P.

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

$$[\mathbf{g}]_\mathbf{P}=([g_1]_{P_1}, [g_2]_{P_2}, ..., [g_n]_{P_n}).$$

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

The following theorem formulates the first main practical result of the present work.

Theorem 2.2. Let $\mathbf{P}=(P_1, P_2,..., P_n)$, $\mathbf{Q}=(Q_1, Q_2,..., Q_n)$, and $\mathbf{K}=(K_1, K_2,..., K_n)$ be n-tuples of natural numbers. Let also A and B be $n \times n$ matrices with natural coefficients such that:

$$\mathbf{Q}^{-1}\cdot A \le \mathbf{K}^{-1},\ \mathbf{P}^{-1}\cdot B \le \mathbf{K}^{-1}.$$

Then for any real vector $\mathbf{g} = (g_1, g_2,\ldots,g_n)$ any integer $n \times n$ matrices $\boldsymbol{a} =(a_{ij})$ and $\boldsymbol{b} =(b_{ij})$ such that $\boldsymbol{a}\cdot\boldsymbol{b} = \boldsymbol{b}\cdot\boldsymbol{a}$ and

$$|a_{ij}|<A_{ij},\ |b_{ij}|<B_{ij}$$

(for all i=1,2,.., n, j=1,2,..,n) 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

$$|\{[\{\mathbf{g}\cdot\boldsymbol{a}\}]_\mathbf{P}\cdot\boldsymbol{b}\}-\{[\{\mathbf{g}\cdot\boldsymbol{b}\}]_\mathbf{Q}\cdot\boldsymbol{a}\}| < \mathbf{K}^{-1}.$$

Therefore, in the latter case,

$$[\{[\{\mathbf{g}\cdot\boldsymbol{a}\}]_\mathbf{P}\}\cdot\boldsymbol{b}]_\mathbf{K} = [\{[\{\mathbf{g}\cdot\boldsymbol{b}\}]_\mathbf{Q}\}\cdot\boldsymbol{a}]_\mathbf{K} + \Delta,$$

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 vector Δ can take 3^n values.

For the proof of *Theorem 2.2* see Appendix B**.**

Rounded Geometric Key Establishment (Rounded GKE) Scheme

Setup

Public *discrete* parameters:

- a natural number n
- two n-tuples of natural numbers $\mathbf{P}=(P_1, P_2,..., P_n)$, $\mathbf{K}=(K_1, K_2,..., K_n)$ as the parameters of rounding
- an n-tuple $\mathbf{M}=(M_0, M_1,..., M_{n-1})$ of natural numbers
- an integer $n\times n$ matrix S

It is required that:

$$\mathbf{P}^{-1}\cdot\mathbf{C}\leq\mathbf{K}^{-1},$$

where

$$\mathbf{C} = M_0\cdot I + M_1\cdot|S| + M_2\cdot|S^2| + \ldots + M_{n-1}\cdot|S^{n-1}|,$$
$$\mathbf{P}^{-1}= (1/P_1, 1/P_2, ..., 1/P_n),\ \mathbf{K}^{-1}= (1/K_1, 1/K_2, ..., 1/K_n).$$

Public *continuous* parameter: an n-tuple of real numbers $\mathbf{g} = (g_1, g_2,\ldots,g_n)$.

Protocol

Alice chooses an n-tuple of secret random integers $a_0, a_1, a_2, \ldots a_{n-1}$ such that

$$|a_0| < M_0, |a_1| < M_1, |a_2| < M_2, \ldots, |a_{n-1}| < M_{n-1},$$

then constructs an integer $n\times n$ matrix $\boldsymbol{a}$ by the formula

$$\boldsymbol{a} = a_0\cdot I + a_1\cdot S + a_2\cdot S^2 + \ldots + a_{n-1}\cdot S^{n-1},$$

then computes the rounded vector $[\{\mathbf{g}\cdot\boldsymbol{a}\}]_{\mathbf{P}}$ and sends it to Bob.

Independently Bob chooses an n-tuple of secret random integers $b_0, b_1, b_2, \ldots b_{n-1}$ such that

$$|b_0| < M_0, |b_1| < M_1, |b_2| < M_2, \ldots, |b_{n-1}| < M_{n-1},$$

and constructs an integer $n\times n$ matrix $\boldsymbol{b}$ by the formula

$$\boldsymbol{b}= b_0\cdot I + b_1\cdot S + b_2\cdot S^2 + \ldots + b_{n-1}\cdot S^{n-1},$$

and computes the rounded vector $[\{\mathbf{g}\cdot\boldsymbol{b}\}]_{\mathbf{P}}$ and sends it to Alice.

Upon receiving the vector $[\{\mathbf{g}\cdot\boldsymbol{b}\}]_{\mathbf{P}}$ from Bob, Alice computes the vector

$$V_A=[\{[\{\mathbf{g}\cdot\boldsymbol{b}\}]_{\mathbf{P}}\cdot\boldsymbol{a}\}]_{\mathbf{K}}.$$

Upon receiving the vector $[\{\mathbf{g}\cdot\boldsymbol{a}\}]_{\mathbf{P}}$ from Alice, Bob computes the vector

$$V_B=[\{[\{\mathbf{g}\cdot\boldsymbol{a}\}]_{\mathbf{P}}\cdot\boldsymbol{b}\}]_{\mathbf{K}}.$$

Common Secret:

By *Theorem 2.2*, one has

$$V_A = V_B + (\varepsilon_1/K_1, \varepsilon_2/K_2, \ldots, \varepsilon_n/K_n),$$

where each ε_i belongs to the set $\{-1, 0, 1\}$. In particular, the difference between V_A and V_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 V_A.

Remark. The idea to eliminate the difference between V_A and V_B using the follow-up communication of Alice and Bob was suggested by Gene Itkis. We express our gratitude to him for this idea.

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
- $\mathbf{M}=(10^8, 10^8)$.
- an integer 2×2 matrix

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

so that

$$a_0\cdot I + a_1\cdot S = \begin{pmatrix} a_0 & -a_1 \\ a_1 & a_0 \end{pmatrix}$$

for any integers a_0, a_1 .

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 **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 **z** to Alice. Upon receiving the vector **y** from Alice, Bob calculates the 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,

$$\mathbf{k}=([\{0.728964042731502072\cdot 19082792+0.16376611710047473 2\cdot 27045821\}]_{\mathbf{K}},$$
$$[\{- 0.728964042731502072\cdot 27045821+ 0.16376611710047473 2\cdot 19082792\}]_{\mathbf{K}})=$$

$$=([\{13910669.202924365887545024+4429189.088964478616694972\}]_{\mathbf{K}},$$
$$[\{-19715431.015152556100441112+3125114.749276002412011744\}]_{\mathbf{K}})$$

$$=(0.2918888445, 0.7341234463)$$

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

Upon receiving the vector **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. Algebro-geometric Key Establishment

In this section we present a key establishment scheme based on our second main example and the general two-sided action key establishment scheme of Section 1. We will refer to it as algebro-geometric key establishment (AGKE).

First, we present the ideal AGKE scheme (i.e., without any rounding involved).

Ideal Algebro-Geometric Key Establishment (AGKE) Scheme

Setup

- m and n are natural numbers ($m\times n$ is the dimension of the scheme).
- $A_m=Mat_m(\mathbb{Z})$ and $A_n=Mat_n(\mathbb{Z})$ are matrix semigroups.
- $X_{m\times n} = Mat_{m\times n}([0,1))$ is the set of all $m\times n$ matrices with coefficients in the semi-open interval [0,1) of the real line (in fact, $X_{m\times n}$ is an $m\times n$ dimensional semi-open unit cube). Each point of $X_{m\times n}$ is an $m\times n$ matrix $\mathbf{g}=(g_{ij})$, where each $g_{ij}\in[0,1)$.
- The maps $A_m\times X_{m\times n} \to X_{m\times n}$ and $X_{m\times n}\times A_n \to X_{m\times n}$ are given respectively by the formulas

  (3.1) $$(\boldsymbol{a},\mathbf{g})\to\{\boldsymbol{a}\cdot\mathbf{g}\},\ (\mathbf{g},\boldsymbol{b})\to\{\mathbf{g}\cdot\boldsymbol{b}\}$$

  for any matrices $\boldsymbol{a}\in A_m$, $\boldsymbol{b}\in A_n$, and any $\mathbf{g}\in X_{m\times n}$, where for each real $m\times n$ matrix $\boldsymbol{x}=(x_{ij})$ we use the notation

  (3.2) $$\{\boldsymbol{x}\}=(\{x_{ij}\}),$$

  where $\{x_{ij}\}$ stands for the fractional part of the real number x_{ij}.

  The following fact is a corollary of *Lemma 1.7*.

Lemma 3.1. The maps $A_m\times X_{m\times n} \to X_{m\times n}$ and $X_{m\times n}\times A_n \to X_{m\times n}$ given by (3.1) constitute a two-sided action of the semigroups $A_m=Mat_m(\mathbb{Z})$ and $A_n=Mat_n(\mathbb{Z})$ on $X_{m\times n} = Mat_{m\times n}([0,1))$. More precisely, for any integer matrices $\boldsymbol{a}\in A_m$, $\boldsymbol{b}\in A_n$, and any $\mathbf{g}\in X_{m\times n}$ one has

(3.3) $$\{\{\boldsymbol{a}\cdot\mathbf{g}\}\cdot\boldsymbol{b}\}=\{\boldsymbol{a}\cdot\mathbf{g}\cdot\boldsymbol{b}\}=\{\boldsymbol{a}\cdot\{\mathbf{g}\cdot\boldsymbol{b}\}\}\ .$$

Proof. In order to reduce the statement to *Lemma 1.7* 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

1. Two communicating parties (let us call them Alice and Bob) choose a non-secret $m\times n$ matrix $\mathbf{g}$ in $X_{m\times n}$.
2. Alice chooses a secret integer $m\times m$ matrix $\boldsymbol{a}$, and Bob independently chooses a secret integer $n\times n$ matrix $\boldsymbol{b}$.
3. Alice computes the $m\times n$ matrix $\{\boldsymbol{a}\cdot\mathbf{g}\}$ and sends it to Bob via an open channel.
4. Bob independently computes the $m\times n$ matrix $\{\mathbf{g}\cdot\boldsymbol{b}\}$ and sends it to Alice via an open channel.
5. Alice computes the $m\times n$ matrix $\boldsymbol{k}_1=\{\boldsymbol{a}\cdot\{\mathbf{g}\cdot\boldsymbol{b}\}\}$; and Bob computes the $m\times n$ matrix $\boldsymbol{k}_2=\{\{\boldsymbol{a}\cdot\mathbf{g}\}\cdot\boldsymbol{b}\}$.

The matrices $\boldsymbol{k}_1$and $\boldsymbol{k}_2$ are equal and therefore constitute the secret shared by Alice and Bob. The equality of the matrices follows from the formula (3.3) above.

Now we present the main example of this section– *rounded* AGKE. Below we will use the following notation.

For any real $m\times n$ matrices $\boldsymbol{y}=(y_{ij})$ and $\boldsymbol{z}=(y_{ij})$, the matrix inequality $\boldsymbol{y}\le\boldsymbol{z}$ 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 $|\boldsymbol{y}|<\boldsymbol{z}$ means that $\boldsymbol{y}<\boldsymbol{z}$ and $-\boldsymbol{y}<\boldsymbol{z}$.

As in Section 2, for any real number $g\in[0,1)$ and any natural number P denote:

$$[g]_P=(\mathrm{Round}(gP))/P$$

if $\mathrm{Round}(gP)<P$, and

$$[g]_P=0$$

if $\mathrm{Round}(gP)=P$.

For an $m\times n$ matrix $\mathbf{P}=(P_{ij})$ of natural numbers and any $m\times n$ matrix $\mathbf{g}=(g_{ij})$ of real numbers such that each $g_{ij}\in[0,1)$, we define the **P**-rounding to a rational $m\times n$ matrix $[\mathbf{g}]_{\mathbf{P}}$ by the formula:

$$[\mathbf{g}]_{\mathbf{P}}=([g_{ij}]_{P_{ij}}).$$

For an $m\times n$ matrix $\mathbf{P}=(P_{ij})$ of natural numbers we denote $\mathbf{P}^*=(1/P_{ij})$.

The following theorem formulates the second main practical result of the present work.

Theorem 3.2. Let be $\mathbf{P}=(P_{ij})$, $\mathbf{Q}=(Q_{ij})$, and $\mathbf{K}=(K_{ij})$ be $m\times n$ matrices of natural numbers. Let $A=(A_{ik})$ be an arbitrary $m\times m$ matrix with natural coefficients and let $B=(B_{lj})$ be an arbitrary $n\times n$ matrix with natural coefficients such that:

$$A\cdot\mathbf{Q}^*\leq \mathbf{K}^*,\ \mathbf{P}^*\cdot B\leq \mathbf{K}^*.$$

Then for any integer $m\times m$ matrix $\boldsymbol{a}$ and any integer $n\times n$ matrix $\boldsymbol{b}$ such that $|\boldsymbol{a}|<A$, $|\boldsymbol{b}|<B$ 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, in the latter case one has

$$\{[\{\boldsymbol{a}\cdot\mathbf{g}\}]_{\mathbf{P}}\cdot\boldsymbol{b}\}_{\mathbf{K}}=\{\boldsymbol{a}\cdot[\{\mathbf{g}\cdot\boldsymbol{b}\}]_{\mathbf{Q}}\}+\Delta,$$

where $\Delta=(\varepsilon_{ij}/K_{ij})$ and where each ε_{ij} belongs to the set $\{-1, 0, 1\}$. In particular, the matrix Δ can take 3^{mn} values.

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

<u>*Rounded Algebro-Geometric Key Establishment (Rounded AGKE) Scheme*</u>

Setup

Public *discrete* parameters:

- natural numbers m and n
- two $m\times n$ matrices of natural numbers $\mathbf{P}=(P_{ij})$, $\mathbf{K}=(K_{ij})$ as the parameters of rounding
- a n-tuple $\mathbf{M}=(M_{ij})$ of natural numbers

It is required that:

$$\mathbf{M}\cdot\mathbf{P}^*\leq \mathbf{K}^*,\ \mathbf{P}^*\cdot\mathbf{M}\leq \mathbf{K}^*.$$

Public *continuous* parameter: an $m\times n$ matrix of real numbers $\mathbf{g}=(g_{ij})$.

Protocol

Alice chooses a secret $m\times m$ matrix $\boldsymbol{a}$ such that $|\boldsymbol{a}|<\mathbf{M}$ then computes the rounded $m\times n$ matrix $[\{\boldsymbol{a}\cdot\mathbf{g}\}]_{\mathbf{P}}$ and sends it to Bob.

Independently Bob chooses a secret $n\times n$ matrix $\boldsymbol{b}$ such that $|\boldsymbol{b}|<\mathbf{M}$ and computes the rounded $m\times n$ matrix $[\{\mathbf{g}\cdot\boldsymbol{b}\}]_{\mathbf{P}}$ and sends it to Alice.

Upon receiving the matrix $[\{\mathbf{g}\cdot\boldsymbol{b}\}]_{\mathbf{P}}$ from Bob, Alice computes the matrix

$$V_A=[\{\boldsymbol{a}\cdot[\{\mathbf{g}\cdot\boldsymbol{b}\}]_{\mathbf{P}}\}]_{\mathbf{K}}.$$

Upon receiving the matrix $[\{\boldsymbol{a}\cdot\mathbf{g}\}]_{\mathbf{P}}$ from Alice, Bob computes the matrix

$$V_B=[\{[\{\boldsymbol{a}\cdot\mathbf{g}\}]_{\mathbf{P}}\cdot\boldsymbol{b}\}]_{\mathbf{K}}.$$

Common Secret:

By *Theorem 3.2*, one has

$$V_A = V_B + (\varepsilon_{ij}/K_{ij}),$$

where each ε_{ij} belongs to the set $\{-1, 0, 1\}$. In particular, the difference between V_A and V_B can take at most 3^{mn} values. This difference can be eliminated in the follow-up communication of Alice and Bob. Thus, the shared secret is the matrix V_A.

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:

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

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

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

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

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

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

$$\boldsymbol{b} = \begin{pmatrix} 691 & 378 \\ 529 & 109 \end{pmatrix}$$

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

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

and sends this 2×2 matrix **z** to Alice. Upon receiving the 2×2 matrix **y** from Alice, Bob calculates the 2×2 matrix **k** =[{**y**·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 **z** from Bob, Alice calculates the 2×2 matrix **k**′=[{***a***·**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 AGKE, 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 5th 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 elements $\boldsymbol{a}\in A$ and $\boldsymbol{b}\in B$ *commute* if

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

for any and $\boldsymbol{x}\in X$.

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

Basic key establishment scheme

Setup:

- a set A
- a set B
- 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 key elements)
- a 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

1. Two communicating parties (let us call them Alice and Bob) choose a shared parameter $\boldsymbol{x}$ of X (this $\boldsymbol{x}$ is not secret).
2. Alice chooses a private (secret) element $\boldsymbol{a}$ in A, and Bob independently chooses a private (secret) element $\boldsymbol{b}$ in B in such a way that $\boldsymbol{a}$ commutes with $\boldsymbol{b}$.
3. Alice computes the transmittable element $\boldsymbol{a}(\boldsymbol{x})$ and Bob independently computes $\boldsymbol{b}(\boldsymbol{x})$.
4. Alice sends the element $\boldsymbol{a}(\boldsymbol{x})$ to Bob via an open channel and Bob sends the element $\boldsymbol{b}(\boldsymbol{x})$ to Alice via an open channel.
5. Alice computes the element $\boldsymbol{k}_A=\boldsymbol{a}(\boldsymbol{b}(\boldsymbol{x}))$ by applying the element $\boldsymbol{a}$ to the received element $\boldsymbol{b}(\boldsymbol{x})$; and Bob computes the element $\boldsymbol{k}_B=\boldsymbol{b}(\boldsymbol{a}(\boldsymbol{x}))$ by applying the element $\boldsymbol{b}$ to the received element $\boldsymbol{a}(\boldsymbol{x})$.

The secret elements $\boldsymbol{k}_A$ and $\boldsymbol{k}_B$ are equal to each other because of (A.1). Therefore, $\boldsymbol{k}_A=\boldsymbol{k}_B$ is the secret shared by Alice and Bob.

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 $\boldsymbol{y} = \boldsymbol{a}(x)$. In the case of the original Diffie-Hellman scheme ([3]), 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.

Based on the rounded schemes introduced in Sections 2 and 3, we propose the 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. [4].

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 set A and a function $f:A\to\mathbb{R}_{>0}$, we say that a map $A\times X \to Y$ is *f-metric* if $d(\boldsymbol{a}(\boldsymbol{x}),\boldsymbol{a}(\boldsymbol{x}')) \leq f(\boldsymbol{a})\cdot d(\boldsymbol{x}, \boldsymbol{x}')$ for any $\boldsymbol{x}, \boldsymbol{x}' \in X$ and $\boldsymbol{a} \in A$ (here we used the standard notation $(\boldsymbol{a}, \boldsymbol{x}) \to \boldsymbol{a}(\boldsymbol{x})$ for the map $A\times X \to Y$).

Definition A.4. Let (X, d) be a metric space. Let K be a discrete subset of X. Consider a map $[\cdot]$: X→K with the property that for each $\boldsymbol{x}\in$X the point $[\boldsymbol{x}]\in$K is the closest to $\boldsymbol{x}$ among all points 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,… be a decreasing sequence of positive real numbers converging to 0. Given an infinite family $[\cdot]_k$: X→X_k of X_k-roundings on (X, d) for k=1,2,… , we say that the family $[\cdot]_k$ is **r**-*saturated* if $d(\boldsymbol{x},[\boldsymbol{x}]_k)\le r_k$ 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, and let $X_1\subset X_2\subset X_3\subset \ldots\subset X_k\subset\ldots$ be an ascending chain of subsets of X. We say that this chain is *uniform* if there exists a sequence $\mathbf{r}=\{r_k\}$ of positive real numbers and a natural number N such that

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

for every $\boldsymbol{x}\in X_k$ and each natural number k. In order to emphasize the dependence of the uniformness on the sequence $\mathbf{r}=\{r_k\}$ and the number N, we will refer to the chain $X_1\subset X_2\subset X_3\subset \ldots\subset X_k\subset\ldots$ as (**r**, N)-*uniform*.

Informally speaking, each (**r**, N)-uniform ascending chain can be used for good approximations of points of X similarly to the way in which rational numbers are used for 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 $\boldsymbol{k}'$ in X_k are *neighbors* if $d(\boldsymbol{k}, \boldsymbol{k}')<r_k$.

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

Theorem A.9. Let A, B, and X be sets, and A×X→ Y_A, B×X→Y_B be maps. Let (Y_A, d), (Y_B, d), and (Z, d) be metric spaces, and let B×Y_A → Z be a g-metric maps, A×Y_B→ Z be a g'-metric map. Also let $[\cdot]_m$: Y_A →$(Y_A)_m$ be an **r**-saturated rounding on (Y_A, d), $[\cdot]'_m$:Y_B →(Y_B)$_m$ be an **r′**-saturated family of roundings on (Y_B, d), and $[\cdot]''_k$:Z →(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:

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

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

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

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

Finally, again by the triangle inequality,

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

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

- a set A
- a set B
- a set X of shared parameters
- an infinite metric space (Y_A, d) of Alice's transmittable elements
- an infinite metric space (Y_B, d) of Bob's transmittable elements
- two maps $A\times X\to Y_A$, $B\times X\to Y_B$
- an $\mathbf{r}$-saturated family of roundings $[\cdot]_m$: $Y_A\to(Y_A)_m$ on (Y_A,d)
- an $\mathbf{r}'$-saturated family of roundings $[\cdot]'_m$: $Y_B\to(Y_B)_m$ on (Y_B,d)
- an infinite metric space (Z, d) of shared key elements
- a g-metric map $B\times Y_A\to Z$
- a g'-metric map $A\times Y_B\to Z$
- 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 $(3\mathbf{r}'',N)$-*uniform*.

Protocol

1. Alice and Bob choose a shared parameter $\boldsymbol{x}\in X$ (this $\boldsymbol{x}$ is not secret) and natural numbers m, k.
2. Alice chooses a private (secret) element $\boldsymbol{a}\in A$, and Bob independently chooses a private (secret) element $\boldsymbol{b}\in B$ in such a way that $\boldsymbol{a}$ commutes with $\boldsymbol{b}$ and $g(\boldsymbol{b})<r''_k/(2r_m)$, $g'(\boldsymbol{a})< r''_k/(2r'_m)$.
3. Alice computes the transmittable element $[\boldsymbol{a}(\boldsymbol{x})]_m$ and Bob independently computes $[\boldsymbol{b}(\boldsymbol{x})]'_m$.
4. Alice sends the element $[\boldsymbol{a}(\boldsymbol{x})]_m$ to Bob via an open channel and Bob sends the element $[\boldsymbol{b}(\boldsymbol{x})]_m$ to Alice via an open channel.
5. Alice computes the element $[\boldsymbol{a}([\boldsymbol{b}(\boldsymbol{x})]'_m)\ ]''_k$ by applying the element $\boldsymbol{a}$ (followed by the rounding $[\cdot]''_k$) to the received element $[\boldsymbol{b}(\boldsymbol{x})]'_m$; and Bob computes the element $[\boldsymbol{b}(\boldsymbol{a}(\boldsymbol{x}))\ ]''_k$ by applying the element $\boldsymbol{b}$ (followed by the rounding $[\cdot]''_k$) to the received element $[\boldsymbol{a}(\boldsymbol{x})]_m$.

According to Theorem A.9, these secret elements are neighbors. Therefore, after making at most N choices, and without revealing the elements they computed, Alice and Bob select $[a([b(x)]'_m)]''_k$ 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,

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

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

By the assumptions, one has:

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

In its turn, the inequality $|\mathbf{E}_1|\le 1/2\cdot\boldsymbol{K}^{-1}$ implies that either the vector $\{\{\mathbf{g}\cdot\boldsymbol{a}\}_{\boldsymbol{P}}\cdot\boldsymbol{b}\}_{\boldsymbol{K}}$ has a coordinate equal to 0 or 1, 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 $|\mathbf{E}_2|\le 1/2\cdot \boldsymbol{K}^{-1}$ implies that either the vector $\{\{\mathbf{g}\cdot\boldsymbol{b}\}_{\boldsymbol{Q}}\cdot\boldsymbol{a}\}_{\boldsymbol{K}}$ has a coordinate equal to 0 or 1, or:

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

Since $\boldsymbol{a}\cdot\boldsymbol{b}=\boldsymbol{b}\cdot\boldsymbol{a}$, one has $\{[\{\mathbf{g}\cdot\boldsymbol{a}\}]_{\mathbf{P}}\cdot\boldsymbol{b}\}-\{[\{\mathbf{g}\cdot\boldsymbol{b}\}]_{\mathbf{Q}}\cdot\boldsymbol{a}\}=\mathbf{E}_1-\mathbf{E}_2$. Note that

$$-\mathbf{K}^{-1}=-1/2\cdot\mathbf{K}^{-1}-1/2\cdot\mathbf{K}^{-1}\le\mathbf{E}_1-\mathbf{E}_2\le 1/2\cdot\mathbf{K}^{-1}-1/2\cdot\mathbf{K}^{-1}=\mathbf{K}^{-1}$$

This finishes the proof. 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

$$-\tfrac{1}{2}\,\mathbf{P}^*\le\theta_1\le\tfrac{1}{2}\,\mathbf{P}^*\text{ and }-\tfrac{1}{2}\,\mathbf{Q}^*\le\theta_2\le\tfrac{1}{2}\,\mathbf{Q}^*.$$

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:

$$|\mathbf{E}_1|=|\theta_1\cdot B|\le 1/2\cdot|\mathbf{P}^*\cdot\boldsymbol{b}|<1/2\cdot\mathbf{P}^*\cdot\beta\le 1/2\cdot\mathbf{K}^*,\ |\mathbf{E}_2|=|\boldsymbol{a}\cdot\theta_2|\le 1/2\cdot|\boldsymbol{a}\cdot\mathbf{Q}^*|<1/2\cdot\mathbf{Q}^*\cdot\alpha\le 1/2\cdot\mathbf{K}^*.$$

In its turn, this implies that either at least one matrix coefficient in $|([\{\boldsymbol{a}\cdot\mathbf{g}\}]_{\mathbf{P}})\cdot\boldsymbol{b}|$ is not greater than the corresponding coefficient of $\tfrac{1}{2}\,\mathbf{K}^*$ or $|([\{\boldsymbol{a}\cdot\mathbf{g}\}]_{\mathbf{P}})\cdot\boldsymbol{b}|>\tfrac{1}{2}\,\mathbf{K}^*$ and:

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

Similarly, the above implies that either at least one matrix coefficient in $|\boldsymbol{a}\cdot([\{\mathbf{g}\cdot\boldsymbol{b}\}]_{\mathbf{Q}})|$ is not greater than the corresponding coefficient of $\tfrac{1}{2}\,\mathbf{K}^*$ or $|\boldsymbol{a}\cdot([\{\mathbf{g}\cdot\boldsymbol{b}\}]_{\mathbf{Q}})|>\tfrac{1}{2}\mathbf{K}^*$ and:

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

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

$$-\tfrac{1}{2}\mathbf{K}^*=-\tfrac{1}{2}\mathbf{K}^*-\tfrac{1}{2}\mathbf{K}^*<\mathbf{E}_1-\mathbf{E}_2<\tfrac{1}{2}\mathbf{K}^*+\tfrac{1}{2}\mathbf{K}^*=\tfrac{1}{2}\mathbf{K}^*.$$

Theorem 3.2 is proved. ■

References

1. I. Anshel, M. Anshel, and D. Goldfeld, "Non-abelian key agreement protocols," Discrete Appl. Math. 130 (2003), no. 1, 3-12.
2. A. Berenstein, L. Chernyak, G. Itkis, ArKE: "Arithmetic Key Establishment System and its Security," preprint.
3. W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transaction on Information Theory vol. IT 22 (November 1976), pp. 644-654.
4. A. Kolmogorov, and S. Fomin, *Introductory real analysis*. Dover Publications, Inc., New York, 1975.
5. 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.