Public key cryptographic algorithms on vector-valued functions

Conference “LOOPS’23”

Fedir Sokhatsky

Vasyl’ Stus Donetsk National University
Vinnytsia, Ukraine

July 1, 2023

Problem:

To build an asymmetric algorithm that is resistant to hacking on an arbitrary computer.

Invertibility of binary operations

Let Q be a set, $\mathcal{O}_2$ the set of all binary operations on Q.

1. the left and right multiplications of binary operations:

$$\left(f \underset{1}{\otimes} g\right)(x,y) := f\left(g(x,y),y\right),$$
$$\left(f \underset{2}{\otimes} g\right)(x,y) := f\left(x,g(x,y)\right);$$

2. the left and right selectors: $e_1(x,y) := x$, $e_2(x,y) := y$;
3. f is called: left (right) invertible if f is an invertible element in the left $(\mathcal{O}_2; \underset{1}{\otimes}, e_1)$ (resp. right $(\mathcal{O}_2; \underset{2}{\otimes}, e_2)$) symmetric monoid; invertible if f is invertible in both left and right symmetric monoids;
4. functional definition: $(Q; f)$ is a quasigroup iff f is invertible.

Invertibility of binary operations

Let Q be a set, $\mathcal{O}_2$ the set of all binary operations on Q.

1. the left and right multiplications of binary operations:

$$\left(f \underset{1}{\otimes} g\right)(x,y) := f\left(g(x,y),y\right),$$
$$\left(f \underset{2}{\otimes} g\right)(x,y) := f\left(x,g(x,y)\right);$$

2. the left and right selectors: $e_1(x,y) := x$, $e_2(x,y) := y$;
3. f is called: left (right) invertible if f is an invertible element in the left $(\mathcal{O}_2; \underset{1}{\otimes}, e_1)$ (resp. right $(\mathcal{O}_2; \underset{2}{\otimes}, e_2)$) symmetric monoid; invertible if f is invertible in both left and right symmetric monoids;
4. functional definition: $(Q; f)$ is a quasigroup iff f is invertible.

Invertibility of binary operations

Let Q be a set, $\mathcal{O}_2$ the set of all binary operations on Q.

1. the left and right multiplications of binary operations:
$$\left(f \underset{1}{\otimes} g\right)(x,y) := f\left(g(x,y),y\right),$$
$$\left(f \underset{2}{\otimes} g\right)(x,y) := f\left(x,g(x,y)\right);$$
2. the left and right selectors: $e_1(x,y) := x$, $e_2(x,y) := y$;
3. f is called: left (right) invertible if f is an invertible element in the left $(\mathcal{O}_2; \underset{1}{\otimes}, e_1)$ (resp. right $(\mathcal{O}_2; \underset{2}{\otimes}, e_2)$) symmetric monoid; invertible if f is invertible in both left and right symmetric monoids;
4. functional definition: $(Q; f)$ is a quasigroup iff f is invertible.

Invertibility of binary operations

Let Q be a set, $\mathcal{O}_2$ the set of all binary operations on Q.

1. the left and right multiplications of binary operations:

$$\left(f \underset{1}{\otimes} g\right)(x,y) := f\left(g(x,y),y\right),$$
$$\left(f \underset{2}{\otimes} g\right)(x,y) := f\left(x,g(x,y)\right);$$

2. the left and right selectors: $e_1(x,y) := x$, $e_2(x,y) := y$;
3. f is called: left (right) invertible if f is an invertible element in the left $(\mathcal{O}_2; \underset{1}{\otimes}, e_1)$ (resp. right $(\mathcal{O}_2; \underset{2}{\otimes}, e_2)$) symmetric monoid; invertible if f is invertible in both left and right symmetric monoids;
4. functional definition: $(Q; f)$ is a quasigroup iff f is invertible.

Invertibility of multiary operations

Let x_i^j be $x_i, \ldots, x_j$, Q be a set, $\mathcal{O}_n$ the set of all n-ary operations on Q.
Then for all $i = 1, \ldots, n$

1. i-th multiplication of n-ary operations and i-th selector:

$$\left(f \underset{i}{\otimes} g\right)(x_1^n) := f\left(x_1^{i-1}, g(x_1^n), x_{i+1}^n\right), \qquad e_i(x_1^n) := x_i;$$

2. i-th symmetric monoid: $(\mathcal{O}_n; \underset{i}{\otimes}, e_i)$;

3. an operation f is called:
   i-invertible if f is an invertible element in i-th symmetric monoid $(\mathcal{O}_n; \underset{i}{\otimes}, e_i)$;
   invertible if f is i-th invertible for all i;

4. functional definition: $(Q; f)$ is a quasigroup iff f is invertible.

Invertibility of multiary operations

Let x_i^j be $x_i, \ldots, x_j$, Q be a set, $\mathcal{O}_n$ the set of all n-ary operations on Q.
Then for all $i = 1, \ldots, n$

1. i-th multiplication of n-ary operations and i-th selector:

$$\left(f \underset{i}{\otimes} g\right)(x_1^n) := f\left(x_1^{i-1}, g(x_1^n), x_{i+1}^n\right), \qquad e_i(x_1^n) := x_i;$$

2. i-th symmetric monoid: $(\mathcal{O}_n; \underset{i}{\otimes}, e_i)$;
3. an operation f is called:
   i-invertible if f is an invertible element in i-th symmetric monoid $(\mathcal{O}_n; \underset{i}{\otimes}, e_i)$;
   invertible if f is i-th invertible for all i;
4. functional definition: $(Q; f)$ is a quasigroup iff f is invertible.

Invertibility of multiary operations

Let x_i^j be $x_i, \ldots, x_j$, Q be a set, $\mathcal{O}_n$ the set of all n-ary operations on Q.
Then for all $i = 1, \ldots, n$

1. i-th multiplication of n-ary operations and i-th selector:

$$\left(f \underset{i}{\otimes} g\right)(x_1^n) := f\left(x_1^{i-1}, g(x_1^n), x_{i+1}^n\right), \qquad e_i(x_1^n) := x_i;$$

2. i-th symmetric monoid: $(\mathcal{O}_n; \underset{i}{\otimes}, e_i)$;
3. an operation f is called:
   i-invertible if f is an invertible element in i-th symmetric monoid $(\mathcal{O}_n; \underset{i}{\otimes}, e_i)$;
   invertible if f is i-th invertible for all i;
4. functional definition: $(Q; f)$ is a quasigroup iff f is invertible.

Invertibility of multiary operations

Let x_i^j be $x_i, \ldots, x_j$, Q be a set, $\mathcal{O}_n$ the set of all n-ary operations on Q.
Then for all $i = 1, \ldots, n$

1. i-th multiplication of n-ary operations and i-th selector:
$$\left(f \underset{i}{\otimes} g\right)(x_1^n) := f\left(x_1^{i-1}, g(x_1^n), x_{i+1}^n\right), \qquad e_i(x_1^n) := x_i;$$
2. i-th symmetric monoid: $(\mathcal{O}_n; \underset{i}{\otimes}, e_i)$;
3. an operation f is called:
   i-invertible if f is an invertible element in i-th symmetric monoid $(\mathcal{O}_n; \underset{i}{\otimes}, e_i)$;
   invertible if f is i-th invertible for all i;
4. functional definition: $(Q; f)$ is a quasigroup iff f is invertible.

Vector-valued operations = vector operations

Vector-valued operations

$g : Q^n \to Q^k$ is a vector-valued operation, n an arity, k a rank. It is also called (m, k)-operation or multioperation.
Example. Let $\mathbb{F}$ be the set of all real numbers. $g : \mathbb{F}^n \to \mathbb{F}^k$. If g is linear, then $g(\bar{x}) = A\bar{x}$ for some matrix A over $\mathbb{F}$.

Coordinate operations

Each of the operations, say g, defines and is defined by a sequence of n-ary operations $g_1, \dots, g_k$:

$$g(x_1^n) = (g_1(x_1^n), \dots, g_k(x_1^n)), \qquad g = (g_1, \dots, g_n).$$

Vector-valued operations = vector operations

Vector-valued operations

$g : Q^n \to Q^k$ is a vector-valued operation, n an arity, k a rank. It is also called (m, k)-operation or multioperation.
Example. Let $\mathbb{F}$ be the set of all real numbers. $g : \mathbb{F}^n \to \mathbb{F}^k$. If g is linear, then $g(\bar{x}) = A\bar{x}$ for some matrix A over $\mathbb{F}$.

Coordinate operations

Each of the operations, say g, defines and is defined by a sequence of n-ary operations $g_1, \ldots, g_k$:

$$g(x_1^n) = (g_1(x_1^n), \ldots, g_k(x_1^n)), \qquad g = (g_1, \ldots, g_n).$$

Symmetric monoids of vector operations

Let Q be a set; $\mathcal{O}_{n,k}$ the set of all n-ary vector-valued operations of the rank $k \leqslant n$; $\varkappa := \{j_1, \ldots, j_k\} \subseteq \{1, \ldots, n\}$; f and g are n-ary vector operations, and $g = (g_1, \ldots, g_k)$.

$\varkappa$-multiplication and $\varkappa$-selector:

$$\left(f \underset{\varkappa}{\otimes} g\right)(x_1^n) = f\left(x_1^{j_1-1}, g_1(x_1^n), x_{j_1+1}^{j_2-1}, \ldots, x_{j_{k-1}+1}^{j_k-1} g_k(x_1^n), x_{j_k+1}^n\right),$$

$$e_\varkappa(x_1, \ldots, x_n) := (x_{j_1}, \ldots, x_{j_k}).$$

$\varkappa$-invertibility

An n-ary vector operation of the rank k is called $\varkappa$-invertible if f is invertible element in the monoid $(\mathcal{O}_{n,k}; \underset{\varkappa}{\otimes}, e_\varkappa)$.

Symmetric monoids of vector operations

Let Q be a set; $\mathcal{O}_{n,k}$ the set of all n-ary vector-valued operations of the rank $k \leqslant n$; $\varkappa := \{j_1, \ldots, j_k\} \subseteq \{1, \ldots, n\}$; f and g are n-ary vector operations, and $g = (g_1, \ldots, g_k)$.

$\varkappa$-multiplication and $\varkappa$-selector:

$$\left(f \underset{\varkappa}{\otimes} g\right)(x_1^n) = f\left(x_1^{j_1-1}, g_1(x_1^n), x_{j_1+1}^{j_2-1}, \ldots, x_{j_{k-1}+1}^{j_k-1} g_k(x_1^n), x_{j_k+1}^n\right),$$
$$e_\varkappa(x_1, \ldots, x_n) := (x_{j_1}, \ldots, x_{j_k}).$$

$\varkappa$-invertibility

An n-ary vector operation of the rank k is called $\varkappa$-invertible if f is invertible element in the monoid $(\mathcal{O}_{n,k}; \underset{\varkappa}{\otimes}, e_\varkappa)$.

Symmetric monoids of vector operations

Let Q be a set; $\mathcal{O}_{n,k}$ the set of all n-ary vector-valued operations of the rank $k \leqslant n$; $\varkappa := \{j_1, \dots, j_k\} \subseteq \{1, \dots, n\}$; f and g are n-ary vector operations, and $g = (g_1, \dots, g_k)$.

$\varkappa$-multiplication and $\varkappa$-selector:

$$\left(f \underset{\varkappa}{\otimes} g\right)(x_1^n) = f\left(x_1^{j_1-1}, g_1(x_1^n), x_{j_1+1}^{j_2-1}, \dots, x_{j_{k-1}+1}^{j_k-1} g_k(x_1^n), x_{j_k+1}^n\right),$$

$$e_\varkappa(x_1, \dots, x_n) := (x_{j_1}, \dots, x_{j_k}).$$

$\varkappa$-invertibility

An n-ary vector operation of the rank k is called $\varkappa$-invertible if f is invertible element in the monoid $(\mathcal{O}_{n,k}; \underset{\varkappa}{\otimes}, e_\varkappa)$.

Construction of $\varkappa$-invertibile vector operations

Definition

Let f be an n-ary vector operation of the rank k on a set Q, $\varkappa \subseteq \{1, \ldots, n\}$ and $k = |\varkappa|$. A transformation of the set Q^k which defined by the term

$$f(x_1, \ldots, x_n) = (y_1, \ldots, y_k)$$

by replacing all $x_i, i \in \varkappa$ with some elements of Q is called a $\varkappa$-translation of f.

Proposition

Each translation of an n-ary $\varkappa$-invertible vector operation of the rank $k = |\varkappa|$ defined on a set Q is a permutation of the set Q^k.

Construction of $\varkappa$-invertibile vector operations

Definition

Let f be an n-ary vector operation of the rank k on a set Q, $\varkappa \subseteq \{1, \dots, n\}$ and $k = |\varkappa|$. A transformation of the set Q^k which defined by the term

$$f(x_1, \dots, x_n) = (y_1, \dots, y_k)$$

by replacing all $x_i, i \in \varkappa$ with some elements of Q is called a $\varkappa$-translation of f.

Proposition

Each translation of an n-ary $\varkappa$-invertible vector operation of the rank $k = |\varkappa|$ defined on a set Q is a permutation of the set Q^k.

The number of invertible multioperations

Proposition

Let $\{\varkappa, \varkappa'\}$ be a partition of $\{1, \ldots, n\}$; $\bar{x}_\varkappa$, $\bar{x}_{\varkappa'}$ be $\varkappa$-subtuples of $(x_1, \ldots, x_n)$, and $\bar{a} \mapsto \lambda_{\bar{a}}$ a mapping of the set Q^{n-k} to the set S_{Q^k} of all permutations of the set Q^k; then f defined by

$$f(x_1, \ldots, x_n) := \lambda_{\bar{x}_{\varkappa'}}(\bar{x}_\varkappa),$$

is an n-ary $\varkappa$-invertible multioperation of the rank $k = |\varkappa|$ on Q.

Corollary

The number of all n-ary $\varkappa$-invertible operations of the rank $k := |\varkappa|$ on an m-element set is

$$\Big((m^k)!\Big)^{m^{n-k}}. \qquad (1)$$

The number of invertible multioperations

Proposition

Let $\{\varkappa, \varkappa'\}$ be a partition of $\{1, \ldots, n\}$; $\bar{x}_\varkappa$, $\bar{x}_{\varkappa'}$ be $\varkappa$-subtuples of $(x_1, \ldots, x_n)$, and $\bar{a} \mapsto \lambda_{\bar{a}}$ a mapping of the set Q^{n-k} to the set S_{Q^k} of all permutations of the set Q^k; then f defined by

$$f(x_1, \ldots, x_n) := \lambda_{\bar{x}_{\varkappa'}}(\bar{x}_\varkappa),$$

is an n-ary $\varkappa$-invertible multioperation of the rank $k = |\varkappa|$ on Q.

Corollary

The number of all n-ary $\varkappa$-invertible operations of the rank $k := |\varkappa|$ on an m-element set is

$$\Big((m^k)!\Big)^{m^{n-k}}. \tag{1}$$

Algorithm

Randomly selection:

- an integer n;
- a partition $\pi := \{\varkappa_1, \dots, \varkappa_s\}$ of the set $\overline{1,n} := \{1, \dots, n\}$;
- n-ary $\varkappa_i$-invertible vector operation f_i of the rank $|\varkappa_i|$ for each $i \in \overline{1,s}$;
- a permutation σ of $\overline{1,n}$ and a permutation τ of $\overline{1,s}$.

Construction:

- the operations $g_1, g_2, \dots, g_s$ on Q by $g_1 := f_1$, and

$$g_i := \left(\dots \left(\left(f_i \underset{\varkappa_{i-1}}{\otimes} f_{i-1} \right) \underset{\varkappa_{i-2}}{\otimes} f_{i-2} \right) \dots \right) \underset{\varkappa_1}{\otimes} f_1, \quad i \in \overline{2,s}, \quad (2)$$

- a transformation θ of Q^n:

$$\theta(x_1^n) := (g_{1\tau}(x_{1\sigma}, x_{2\sigma}, \dots, x_{n\sigma}), \dots, g_{s\tau}(x_{1\sigma}, x_{2\sigma}, \dots, x_{n\sigma})).$$

Randomly selection:

- an integer n;
- a partition $\pi := \{\varkappa_1, \dots, \varkappa_s\}$ of the set $\overline{1,n} := \{1, \dots, n\}$;
- n-ary $\varkappa_i$-invertible vector operation f_i of the rank $|\varkappa_i|$ for each $i \in \overline{1,s}$;
- a permutation σ of $\overline{1,n}$ and a permutation τ of $\overline{1,s}$.

Construction:

- the operations $g_1, g_2, \dots, g_s$ on Q by $g_1 := f_1$, and

$$g_i := \left(\dots \left(\left(f_i \underset{\varkappa_{i-1}}{\otimes} f_{i-1} \right) \underset{\varkappa_{i-2}}{\otimes} f_{i-2} \right) \dots \right) \underset{\varkappa_1}{\otimes} f_1, \quad i \in \overline{2,s}, \quad (2)$$

- a transformation θ of Q^n:

$$\theta(x_1^n) := \left(g_{1\tau}(x_{1\sigma}, x_{2\sigma}, \dots, x_{n\sigma}), \dots, g_{s\tau}(x_{1\sigma}, x_{2\sigma}, \dots, x_{n\sigma})\right).$$

Randomly selection:

- an integer n;
- a partition $\pi := \{\varkappa_1, \ldots, \varkappa_s\}$ of the set $\overline{1,n} := \{1, \ldots, n\}$;
- n-ary $\varkappa_i$-invertible vector operation f_i of the rank $|\varkappa_i|$ for each $i \in \overline{1,s}$;
- a permutation σ of $\overline{1,n}$ and a permutation τ of $\overline{1,s}$.

Construction:

- the operations $g_1, g_2, \ldots, g_s$ on Q by $g_1 := f_1$, and

$$g_i := \left(\ldots \left(\left(f_i \underset{\varkappa_{i-1}}{\otimes} f_{i-1} \right) \underset{\varkappa_{i-2}}{\otimes} f_{i-2} \right) \ldots \right) \underset{\varkappa_1}{\otimes} f_1, \quad i \in \overline{2,s}, \quad (2)$$

- a transformation θ of Q^n:

$$\theta(x_1^n) := \left(g_{1\tau}(x_{1\sigma}, x_{2\sigma}, \ldots, x_{n\sigma}), \ldots, g_{s\tau}(x_{1\sigma}, x_{2\sigma}, \ldots, x_{n\sigma}) \right).$$

Algorithm

Randomly selection:

- an integer n;
- a partition $\pi := \{\varkappa_1, \dots, \varkappa_s\}$ of the set $\overline{1,n} := \{1, \dots, n\}$;
- n-ary $\varkappa_i$-invertible vector operation f_i of the rank $|\varkappa_i|$ for each $i \in \overline{1,s}$;
- a permutation σ of $\overline{1,n}$ and a permutation τ of $\overline{1,s}$.

Construction:

- the operations $g_1, g_2, \dots, g_s$ on Q by $g_1 := f_1$, and

$$g_i := \left(\dots\left(\left(f_i \underset{\varkappa_{i-1}}{\otimes} f_{i-1}\right) \underset{\varkappa_{i-2}}{\otimes} f_{i-2}\right)\dots\right) \underset{\varkappa_1}{\otimes} f_1, \quad i \in \overline{2,s}, \quad (2)$$

- a transformation θ of Q^n:

$$\theta(x_1^n) := (g_{1\tau}(x_{1\sigma}, x_{2\sigma}, \dots, x_{n\sigma}), \dots, g_{s\tau}(x_{1\sigma}, x_{2\sigma}, \dots, x_{n\sigma})).$$

Algorithm

Randomly selection:

- an integer n;
- a partition $\pi := \{\varkappa_1, \dots, \varkappa_s\}$ of the set $\overline{1,n} := \{1, \dots, n\}$;
- n-ary $\varkappa_i$-invertible vector operation f_i of the rank $|\varkappa_i|$ for each $i \in \overline{1,s}$;
- a permutation σ of $\overline{1,n}$ and a permutation τ of $\overline{1,s}$.

Construction:

- the operations $g_1, g_2, \dots, g_s$ on Q by $g_1 := f_1$, and

$$g_i := \left(\dots\left(\left(f_i \underset{\varkappa_{i-1}}{\otimes} f_{i-1}\right) \underset{\varkappa_{i-2}}{\otimes} f_{i-2}\right)\dots\right) \underset{\varkappa_1}{\otimes} f_1, \quad i \in \overline{2,s}, \quad (2)$$

- a transformation θ of Q^n:

$$\theta(x_1^n) := \left(g_{1\tau}(x_{1\sigma}, x_{2\sigma}, \dots, x_{n\sigma}), \dots, g_{s\tau}(x_{1\sigma}, x_{2\sigma}, \dots, x_{n\sigma})\right).$$

Algorithm

Randomly selection:

- an integer n;
- a partition $\pi := \{\varkappa_1, \dots, \varkappa_s\}$ of the set $\overline{1,n} := \{1, \dots, n\}$;
- n-ary $\varkappa_i$-invertible vector operation f_i of the rank $|\varkappa_i|$ for each $i \in \overline{1,s}$;
- a permutation σ of $\overline{1,n}$ and a permutation τ of $\overline{1,s}$.

Construction:

- the operations $g_1, g_2, \dots, g_s$ on Q by $g_1 := f_1$, and

$$g_i := \left(\dots \left(\left(f_i \underset{\varkappa_{i-1}}{\otimes} f_{i-1} \right) \underset{\varkappa_{i-2}}{\otimes} f_{i-2} \right) \dots \right) \underset{\varkappa_1}{\otimes} f_1, \quad i \in \overline{2,s}, \quad (2)$$

- a transformation θ of Q^n:

$$\theta(x_1^n) := \big(g_{1\tau}(x_{1\sigma}, x_{2\sigma}, \dots, x_{n\sigma}), \dots, g_{s\tau}(x_{1\sigma}, x_{2\sigma}, \dots, x_{n\sigma})\big).$$

Algorithm

Keys:

- Public key: the pair (n, θ).
- Private key: the sequence of all other parameters: π, $f_1, \ldots, f_s$, s, σ, τ.

Action of the algorithm

Let $\mathcal{I}$ be the information sequence of the alphabet Q that Bob is going to send to Alice.

1. Alice creates the pair (n, θ) and sends it to Bob;
2. Bob divides the sequence $\mathcal{I}$ into vectors of the length n, applies θ to each of them, and sends the received sequence to Alice;
3. Alice decrypts the ciphertext using the privat key.

Keys:

- Public key: the pair (n, θ).
- Private key: the sequence of all other parameters: π, $f_1, \ldots,$ f_s, s, σ, τ.

Action of the algorithm

Let $\mathcal{I}$ be the information sequence of the alphabet Q that Bob is going to send to Alice.

1. Alice creates the pair (n, θ) and sends it to Bob;
2. Bob divides the sequence $\mathcal{I}$ into vectors of the length n, applies θ to each of them, and sends the received sequence to Alice;
3. Alice decrypts the ciphertext using the privat key.

Algorithm

Keys:

- Public key: the pair (n, θ).
- Private key: the sequence of all other parameters: π, f_1, $\ldots$, f_s, s, σ, τ.

Action of the algorithm

Let $\mathcal{I}$ be the information sequence of the alphabet Q that Bob is going to send to Alice.

1. Alice creates the pair (n, θ) and sends it to Bob;
2. Bob divides the sequence $\mathcal{I}$ into vectors of the length n, applies θ to each of them, and sends the received sequence to Alice;
3. Alice decrypts the ciphertext using the privat key.

Algorithm

Keys:

- Public key: the pair (n, θ).
- Private key: the sequence of all other parameters: π, f_1, ..., f_s, s, σ, τ.

Action of the algorithm

Let $\mathcal{I}$ be the information sequence of the alphabet Q that Bob is going to send to Alice.

1. Alice creates the pair (n, θ) and sends it to Bob;
2. Bob divides the sequence $\mathcal{I}$ into vectors of the length n, applies θ to each of them, and sends the received sequence to Alice;
3. Alice decrypts the ciphertext using the privat key.

Algorithm

Keys:

- Public key: the pair (n, θ).
- Private key: the sequence of all other parameters: π, f_1, $\dots$, f_s, s, σ, τ.

Action of the algorithm

Let $\mathcal{I}$ be the information sequence of the alphabet Q that Bob is going to send to Alice.

1. Alice creates the pair (n, θ) and sends it to Bob;
2. Bob divides the sequence $\mathcal{I}$ into vectors of the length n, applies θ to each of them, and sends the received sequence to Alice;
3. Alice decrypts the ciphertext using the privat key.

Algorithm

Keys:

- Public key: the pair (n, θ).
- Private key: the sequence of all other parameters: π, f_1, ..., f_s, s, σ, τ.

Action of the algorithm

Let $\mathcal{I}$ be the information sequence of the alphabet Q that Bob is going to send to Alice.

1. Alice creates the pair (n, θ) and sends it to Bob;
2. Bob divides the sequence $\mathcal{I}$ into vectors of the length n, applies θ to each of them, and sends the received sequence to Alice;
3. Alice decrypts the ciphertext using the privat key.

Algorithm

Keys:

- Public key: the pair (n, θ).
- Private key: the sequence of all other parameters: π, f_1, $\ldots$, f_s, s, σ, τ.

Action of the algorithm

Let $\mathcal{I}$ be the information sequence of the alphabet Q that Bob is going to send to Alice.

1. Alice creates the pair (n, θ) and sends it to Bob;
2. Bob divides the sequence $\mathcal{I}$ into vectors of the length n, applies θ to each of them, and sends the received sequence to Alice;
3. Alice decrypts the ciphertext using the privat key.

Example

Suppose that a computer makes 10^c calculations per second and one calculation is one cipher check (for today's fastest computer $c < 19$). Let

$$m = 2 \text{ (cardinality of the alphabet } Q\text{)},$$
$$n = 20 \text{ (arity of the vector operations)},$$
$$s = 5 \text{ (the number of classes } \varkappa_i \text{ in the partition of } \{1, \ldots, 20\}\text{)},$$
$$|\varkappa_1| = 2, \quad |\varkappa_2| = 3, \quad |\varkappa_3| = 4, \quad |\varkappa_4| = 5, \quad |\varkappa_5| = 6.$$

The brute force attack

To consider all possibilities, the computer needs more than $10^{3\,000\,000-c}$ years.

Example

Suppose that a computer makes 10^c calculations per second and one calculation is one cipher check (for today's fastest computer $c < 19$). Let

$$m = 2 \text{ (cardinality of the alphabet } Q\text{)},$$
$$n = 20 \text{ (arity of the vector operations)},$$
$$s = 5 \text{ (the number of classes } \varkappa_i \text{ in the partition of } \{1, \dots, 20\}\text{)},$$
$$|\varkappa_1| = 2, \quad |\varkappa_2| = 3, \quad |\varkappa_3| = 4, \quad |\varkappa_4| = 5, \quad |\varkappa_5| = 6.$$

The brute force attack

To consider all possibilities, the computer needs more than $10^{3\,000\,000-c}$ years.

Example

Suppose that a computer makes 10^c calculations per second and one calculation is one cipher check (for today's fastest computer $c < 19$). Let

$$m = 2 \text{ (cardinality of the alphabet } Q\text{)},$$
$$n = 20 \text{ (arity of the vector operations)},$$
$$s = 5 \text{ (the number of classes } \varkappa_i \text{ in the partition of } \{1, \dots, 20\}\text{)},$$
$$|\varkappa_1| = 2, \quad |\varkappa_2| = 3, \quad |\varkappa_3| = 4, \quad |\varkappa_4| = 5, \quad |\varkappa_5| = 6.$$

The brute force attack

To consider all possibilities, the computer needs more than $10^{3\,000\,000-c}$ years.

Thank you for your attention!