Linear Weaknesses in T-functions

Tao Shi,[1] Vladimir Anashin[2] and Dongdai Lin [1]

[1]State Key Laboratory of Information Security
Institute of Information Engineering Chinese Academy of Sciences
[2]Faculty of Computational Mathematics and Cybernetics
Lomonosov Moscow State University

Outline

T-functions

Loosely speaking, a T-function on k-bit words is a map of k-bit words into k-bit words such that each i-th bit of image depends only on low-order bits $0, ..., i$ of the pre-image. Formally, a (univariate) T-function f is a mapping

$$\dots ; \chi_2 ; \chi_1 ; \chi_0 \overset{f}{\mapsto} \dots , \psi_2(\chi_0, \chi_1, \chi_2) ; \psi_1(\chi_0, \chi_1) ; \psi_0(\chi_0)$$

where $\chi_i \in \{0, 1\}$, and each $\psi_i(\chi_0, \dots, \chi_i)$ is a Boolean function in Boolean variables $\chi_0, \dots, \chi_i$.

As any bit word may be regarded as a base-2 expansion of a non-negative integer, T-functions may be considered as maps from integers to integers.

The determinative property of T-functions (which might be used to state an equivalent definition of a T-function) is compatibility with all congruences modulo powers of 2: Given a (univariate) T-function f, if $a \equiv b \pmod{2^s}$ then $f(a) \equiv f(b) \pmod{2^s}$. Vice versa, every compatible map is a T-function.

T-functions

Loosely speaking, a T-function on k-bit words is a map of k-bit words into k-bit words such that each i-th bit of image depends only on low-order bits $0, ..., i$ of the pre-image. Formally, a (univariate) T-function f is a mapping

$$\ldots; \chi_2; \chi_1; \chi_0 \stackrel{f}{\mapsto} \ldots, \psi_2(\chi_0, \chi_1, \chi_2); \psi_1(\chi_0, \chi_1); \psi_0(\chi_0)$$

where $\chi_i \in \{0, 1\}$, and each $\psi_i(\chi_0, \ldots, \chi_i)$ is a Boolean function in Boolean variables $\chi_0, \ldots, \chi_i$.

As any bit word may be regarded as a base-2 expansion of a non-negative integer, T-functions may be considered as maps from integers to integers.

The determinative property of T-functions (which might be used to state an equivalent definition of a T-function) is compatibility with all congruences modulo powers of 2: Given a (univariate) T-function f, if $a \equiv b \pmod{2^s}$ then $f(a) \equiv f(b) \pmod{2^s}$. Vice versa, every compatible map is a T-function.

T-functions

Loosely speaking, a T-function on k-bit words is a map of k-bit words into k-bit words such that each i-th bit of image depends only on low-order bits $0, ..., i$ of the pre-image. Formally, a (univariate) T-function f is a mapping

$$\ldots;\chi_2;\chi_1;\chi_0 \stackrel{f}{\mapsto} \ldots,\psi_2(\chi_0,\chi_1,\chi_2);\psi_1(\chi_0,\chi_1);\psi_0(\chi_0)$$

where $\chi_i \in \{0,1\}$, and each $\psi_i(\chi_0,\ldots,\chi_i)$ is a Boolean function in Boolean variables $\chi_0,\ldots,\chi_i$.

As any bit word may be regarded as a base-2 expansion of a non-negative integer, T-functions may be considered as maps from integers to integers.

The determinative property of T-functions (which might be used to state an equivalent definition of a T-function) is compatibility with all congruences modulo powers of 2: Given a (univariate) T-function f, if $a \equiv b \pmod{2^s}$ then $f(a) \equiv f(b) \pmod{2^s}$. Vice versa, every compatible map is a T-function.

T-functions in cryptography

Important examples of T-functions are basic machine instructions: integer arithmetic operations (addition, multiplication,...); bitwise logical operations ($\vee$, $\oplus$, $\wedge$, $\neg$); some of their compositions (masking, shifts towards high order bits, reduction modulo 2^k). A composition of T-functions is a T-function (for instance, *any polynomial with integer coefficients is a T-function*).

That is why T-functions were found to be useful tools to design fast cryptographic primitives and ciphers based on usage of both arithmetic (addition, multiplication) and logical operations. Various methods are known to construct transitive T-functions (the ones that produce sequences of the longest possible period, 2^k). Transitive T-functions have been considered as a candidate to replace LFSRs in keystream generators of stream ciphers. since sequences produced by T-function-based keystream generators are proved to have a number of good cryptographic properties, such as high linear and 2-adic complexity, uniform distribution of subwords, etc.

T-functions in cryptography

Important examples of T-functions are basic machine instructions: integer arithmetic operations (addition, multiplication,...); bitwise logical operations ($\vee$, $\oplus$, $\wedge$, $\neg$); some of their compositions (masking, shifts towards high order bits, reduction modulo 2^k). A composition of T-functions is a T-function (for instance, *any polynomial with integer coefficients is a T-function*).

That is why T-functions were found to be useful tools to design fast cryptographic primitives and ciphers based on usage of both arithmetic (addition, multiplication) and logical operations. Various methods are known to construct transitive T-functions (the ones that produce sequences of the longest possible period, 2^k). Transitive T-functions have been considered as a candidate to replace LFSRs in keystream generators of stream ciphers. since sequences produced by T-function-based keystream generators are proved to have a number of good cryptographic properties, such as high linear and 2-adic complexity, uniform distribution of subwords, etc.

T-functions in cryptography

Important examples of T-functions are basic machine instructions: integer arithmetic operations (addition, multiplication,...); bitwise logical operations ($\vee$, $\oplus$, $\wedge$, $\neg$); some of their compositions (masking, shifts towards high order bits, reduction modulo 2^k). A composition of T-functions is a T-function (for instance, *any polynomial with integer coefficients is a T-function*).

That is why T-functions were found to be useful tools to design fast cryptographic primitives and ciphers based on usage of both arithmetic (addition, multiplication) and logical operations. Various methods are known to construct transitive T-functions (the ones that produce sequences of the longest possible period, 2^k). Transitive T-functions have been considered as a candidate to replace LFSRs in keystream generators of stream ciphers. since sequences produced by T-function-based keystream generators are proved to have a number of good cryptographic properties, such as high linear and 2-adic complexity, uniform distribution of subwords, etc.

T-functions in cryptography

Important examples of T-functions are basic machine instructions: integer arithmetic operations (addition, multiplication,...); bitwise logical operations ($\vee$, $\oplus$, $\wedge$, $\neg$); some of their compositions (masking, shifts towards high order bits, reduction modulo 2^k). A composition of T-functions is a T-function (for instance, *any polynomial with integer coefficients is a T-function*).

That is why T-functions were found to be useful tools to design fast cryptographic primitives and ciphers based on usage of both arithmetic (addition, multiplication) and logical operations. Various methods are known to construct transitive T-functions (the ones that produce sequences of the longest possible period, 2^k). Transitive T-functions have been considered as a candidate to replace LFSRs in keystream generators of stream ciphers. since sequences produced by T-function-based keystream generators are proved to have a number of good cryptographic properties, such as high linear and 2-adic complexity, uniform distribution of subwords, etc.

Coordinate sequences

Given a transitive T-function f, we consider a k-bit word sequence $x_0, x_1, \ldots$ produced by f with respect to the recurrence law

$$x_i = f(x_{i-1}) = f^i(x_0) = \underbrace{f(\ldots(f(}_{i}x_0)\ldots), \qquad i = 0, 1, 2, \ldots,$$

(by the definition, $f^0(x_0) = x_0$), and denote by $\delta_n(x_i)$ the n-th bit of the word x_i, $n = 0, 1, \ldots, k-1$.

- The n-th coordinate sequence is the bit sequence

$$\delta_n(x_0), \delta_n(x_1), \delta_n(x_2) \ldots$$

Coordinate sequences

Given a transitive T-function f, we consider a k-bit word sequence $x_0, x_1, \ldots$ produced by f with respect to the recurrence law

$$x_i = f(x_{i-1}) = f^i(x_0) = \underbrace{f(\ldots(f(}_{i}x_0)\ldots), \qquad i = 0, 1, 2, \ldots,$$

(by the definition, $f^0(x_0) = x_0$), and denote by $\delta_n(x_i)$ the n-th bit of the word x_i, $n = 0, 1, \ldots, k-1$.

- The n-th coordinate sequence is the bit sequence

$$\delta_n(x_0), \delta_n(x_1), \delta_n(x_2) \ldots$$

Known results

Molland and Helleseth (2005) discovered that for the transitive T-function $f(x) = x + (x^2 \vee C)$ suggested by Klimov and Shamir (2003), adjacent coordinate sequences satisfy linear relation of the form

$$\delta_n(x_{i+2^{n-1}}) \equiv \delta_n(x_i) + \delta_{n-1}(x_i) + z_i \pmod 2, \text{ for all } i = 0, 1, 2, \dots,$$

where the length of the period of the sequence z_i is only 4 (and *not* 2^n as in a general case, for an arbitrary transitive T-function); Jin-Song Wang and Wen-Feng Qi (2008) obtained similar result for a transitive polynomial function $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_m x^m$ with integer coefficients $c_0, c_1, \ldots \in \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$.

Known results

Molland and Helleseth (2005) discovered that for the transitive T-function $f(x) = x + (x^2 \vee C)$ suggested by Klimov and Shamir (2003), adjacent coordinate sequences satisfy linear relation of the form

$$\delta_n(x_{i+2^{n-1}}) \equiv \delta_n(x_i) + \delta_{n-1}(x_i) + z_i \pmod 2, \text{ for all } i = 0, 1, 2, \ldots,$$

where the length of the period of the sequence z_i is only 4 (and *not* 2^n as in a general case, for an arbitrary transitive T-function); Jin-Song Wang and Wen-Feng Qi (2008) obtained similar result for a transitive polynomial function $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_m x^m$ with integer coefficients $c_0, c_1, \ldots \in \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$.

Our contribution

- Firstly, we prove that the linear relation

$$\delta_n(x_{i+2^{n-1}}) \equiv \delta_n(x_i) + \delta_{n-1}(x_i) + z_i \pmod 2;\ i = 0, 1, 2, \dots$$

holds for a much wider class of T-functions than polynomials over $\mathbb{Z}$ and Klimov-Shamir functions $f(x) = x + (x^2 \vee C)$, $C \in \mathbb{Z}$. This wider class contains exponential T-functions (such as $f(x) = 3x + 3^x$), fractional T-functions (such as $f(x) = 1 + x + \frac{4}{1+2x}$) and many other T-functions that might be extremely complex compositions of numerical and logical operators.

The length of the period of the binary sequence z_i in the relation depends on the function f and is not necessarily 4 any longer. However, the length is still short and does not depend on the order n of coordinate sequence.

Our contribution

- Firstly, we prove that the linear relation

$$\delta_n(x_{i+2^{n-1}}) \equiv \delta_n(x_i) + \delta_{n-1}(x_i) + z_i \pmod 2; \; i = 0, 1, 2, \ldots$$

holds for a much wider class of T-functions than polynomials over $\mathbb{Z}$ and Klimov-Shamir functions $f(x) = x + (x^2 \vee C)$, $C \in \mathbb{Z}$. This wider class contains exponential T-functions (such as $f(x) = 3x + 3^x$), fractional T-functions (such as $f(x) = 1+x+\frac{4}{1+2x}$) and many other T-functions that might be extremely complex compositions of numerical and logical operators.

The length of the period of the binary sequence z_i in the relation depends on the function f and is not necessarily 4 any longer. However, the length is still short and does not depend on the order n of coordinate sequence.

Our contribution

- Secondly, for a slightly narrower class of T-functions than the previous one, we prove that a quadratic relation holds for any three consecutive coordinate sequences. Earlier a relation of this sort was known only for Klimov-Shamir T-function.

Both linear and quadratic relations we discuss may be used to construct attacks against some T-function-based stream ciphers, and moreover, against stream ciphers based on multiword T-functions (such as TSC) as well as the ones that T-function-based counter-dependent generators (such as ABC). We obtain our results by using techniques of non-Archimedean dynamics; that is, we expand T-functions onto the whole space $\mathbb{Z}_2$ of 2-adic integers and study corresponding dynamical systems.

Our contribution

- Secondly, for a slightly narrower class of T-functions than the previous one, we prove that a quadratic relation holds for any three consecutive coordinate sequences. Earlier a relation of this sort was known only for Klimov-Shamir T-function.

Both linear and quadratic relations we discuss may be used to construct attacks against some T-function-based stream ciphers, and moreover, against stream ciphers based on multiword T-functions (such as TSC) as well as the ones that T-function-based counter-dependent generators (such as ABC).
We obtain our results by using techniques of non-Archimedean dynamics; that is, we expand T-functions onto the whole space $\mathbb{Z}_2$ of 2-adic integers and study corresponding dynamical systems.

Our contribution

- Secondly, for a slightly narrower class of T-functions than the previous one, we prove that a quadratic relation holds for any three consecutive coordinate sequences. Earlier a relation of this sort was known only for Klimov-Shamir T-function.

Both linear and quadratic relations we discuss may be used to construct attacks against some T-function-based stream ciphers, and moreover, against stream ciphers based on multiword T-functions (such as TSC) as well as the ones that T-function-based counter-dependent generators (such as ABC). We obtain our results by using techniques of non-Archimedean dynamics; that is, we expand T-functions onto the whole space $\mathbb{Z}_2$ of 2-adic integers and study corresponding dynamical systems.

2-adic integers

From the definition, any T-function is well-defined on the set $\mathbb{Z}_2$ of all infinite binary sequences $\ldots\delta_2(x)\delta_1(x)\delta_0(x) = x$, where $\delta_j(x) \in \{0,1\}$, $j = 0,1,2,\ldots$.

Arithmetic operations (addition and multiplication) with these sequences could be defined via standard "school-textbook" algorithms of addition and multiplication of natural numbers represented by base-2 expansions. The ring $\mathbb{Z}_2$ is commutative with respect to the so defined addition and multiplication, and is called the ring of 2-adic integers

2-adic integers

From the definition, any T-function is well-defined on the set $\mathbb{Z}_2$ of all infinite binary sequences $\ldots\delta_2(x)\delta_1(x)\delta_0(x) = x$, where $\delta_j(x) \in \{0,1\}$, $j = 0, 1, 2, \ldots$.

Arithmetic operations (addition and multiplication) with these sequences could be defined via standard "school-textbook" algorithms of addition and multiplication of natural numbers represented by base-2 expansions.The ring $\mathbb{Z}_2$ is commutative with respect to the so defined addition and multiplication, and is called the ring of 2-adic integers

2-adic metric

The ring $\mathbb{Z}_2$ is a metric space: A distance (=metric) $d(a,b)$ between $a,b \in \mathbb{Z}_2$ is 2^{-l}, where $l =$(the length of the longest common prefix of a and b). Absolute value of $a \in \mathbb{Z}_2$ is a distance from a to 0: $|a|_2 = d(a,0)$; so $d(a,b) = |a-b|_2$. The metric d is non-Archimedean; that is, satisfies the strong triangle inequality: for all $a,b,c \in \mathbb{Z}_2$

$$|a-b|_2 \le \max\{|a-c|_2, |c-b|_2\},$$

Formally, the ring $\mathbb{Z}_2$ could be defined as a completion of the ring $\mathbb{Z}$ with respect to this non-Archimedean metric.

Now, we represent every 2-adic integer $x = \ldots\delta_2(x)\delta_1(x)\delta_0(x)$ (where $\delta_i(x) \in \{0,1\}, i = 0,1,2,\ldots$) as the series $x = \sum_{i=0}^{\infty} \delta_i(x) \cdot 2^i$; (where $\delta_i(x) \in \{0,1\}, i = 0,1,2,\ldots$). The series are called canonic 2-adic expansion of the 2-adic integer x; the series converges to x with respect to the 2-adic metric.

2-adic metric

The ring $\mathbb{Z}_2$ is a metric space: A distance (=metric) $d(a,b)$ between $a, b \in \mathbb{Z}_2$ is 2^{-l}, where l =(the length of the longest common prefix of a and b). Absolute value of $a \in \mathbb{Z}_2$ is a distance from a to 0: $|a|_2 = d(a,0)$; so $d(a,b) = |a-b|_2$. The metric d is non-Archimedean; that is, satisfies the strong triangle inequality: for all $a, b, c \in \mathbb{Z}_2$

$$|a-b|_2 \leq \max\{|a-c|_2, |c-b|_2\},$$

Formally, the ring $\mathbb{Z}_2$ could be defined as a completion of the ring $\mathbb{Z}$ with respect to this non-Archimedean metric.

Now, we represent every 2-adic integer $x = \ldots\delta_2(x)\delta_1(x)\delta_0(x)$ (where $\delta_i(x) \in \{0,1\}, i = 0,1,2,\ldots$) as the series $x = \sum_{i=0}^{\infty} \delta_i(x) \cdot 2^i$; (where $\delta_i(x) \in \{0,1\}, i = 0,1,2,\ldots$). The series are called canonic 2-adic expansion of the 2-adic integer x; the series converges to x with respect to the 2-adic metric.

2-adic metric

The ring $\mathbb{Z}_2$ is a metric space: A distance (=metric) $d(a,b)$ between $a,b \in \mathbb{Z}_2$ is 2^{-l}, where $l =$(the length of the longest common prefix of a and b). Absolute value of $a \in \mathbb{Z}_2$ is a distance from a to 0: $|a|_2 = d(a,0)$; so $d(a,b) = |a-b|_2$. The metric d is non-Archimedean; that is, satisfies the strong triangle inequality: for all $a,b,c \in \mathbb{Z}_2$

$$|a-b|_2 \leq \max\{|a-c|_2, |c-b|_2\},$$

Formally, the ring $\mathbb{Z}_2$ could be defined as a completion of the ring $\mathbb{Z}$ with respect to this non-Archimedean metric.

Now, we represent every 2-adic integer $x = \ldots\delta_2(x)\delta_1(x)\delta_0(x)$ (where $\delta_i(x) \in \{0,1\}$, $i = 0,1,2,\ldots$) as the series $x = \sum_{i=0}^{\infty} \delta_i(x) \cdot 2^i$; (where $\delta_i(x) \in \{0,1\}, i = 0,1,2,\ldots$). The series are called canonic 2-adic expansion of the 2-adic integer x; the series converges to x with respect to the 2-adic metric.

T-functions are 2-adic maps

T-functions may be viewed as mappings from 2-adic integers to 2-adic integers: e.g., for a univariate T-function f

$$\chi_0+\chi_1\cdot 2+\chi_2\cdot 2^2+\cdots \stackrel{f}{\mapsto} \psi_0(\chi_0)+\psi_1(\chi_0,\chi_1)\cdot 2+\psi_2(\chi_0,\chi_1,\chi_2)\cdot 2^2+\cdots .$$

We refer to these Boolean functions $\psi_0, \psi_1, \psi_2, \ldots$ as coordinate functions of the T-function f.

If the T-functions are restricted to the set of all numbers whose base-2 expansions are not longer than k, we sometimes refer to these restrictions as T-functions on k-bit words: We usually associate the set of all k-bit words to the set $\{0, 1, \ldots, 2^k - 1\}$ of all residues modulo 2^k; the latter set constitutes the residue ring $\mathbb{Z}/2^k\mathbb{Z}$ modulo 2^k w.r.t. modulo 2^k operations of addition and multiplication.

T-functions are 2-adic maps

T-functions may be viewed as mappings from 2-adic integers to 2-adic integers: e.g., for a univariate T-function f

$$\chi_0+\chi_1\cdot 2+\chi_2\cdot 2^2+\cdots \stackrel{f}{\mapsto} \psi_0(\chi_0)+\psi_1(\chi_0,\chi_1)\cdot 2+\psi_2(\chi_0,\chi_1,\chi_2)\cdot 2^2+\cdots .$$

We refer to these Boolean functions $\psi_0,\psi_1,\psi_2,\ldots$ as coordinate functions of the T-function f.

If the T-functions are restricted to the set of all numbers whose base-2 expansions are not longer than k, we sometimes refer to these restrictions as T-functions on k-bit words: We usually associate the set of all k-bit words to the set $\{0,1,\ldots,2^k-1\}$ of all residues modulo 2^k; the latter set constitutes the residue ring $\mathbb{Z}/2^k\mathbb{Z}$ modulo 2^k w.r.t. modulo 2^k operations of addition and multiplication.

T-functions are 2-adic maps

T-functions may be viewed as mappings from 2-adic integers to 2-adic integers: e.g., for a univariate T-function f

$$\chi_0+\chi_1\cdot 2+\chi_2\cdot 2^2+\cdots \overset{f}{\mapsto} \psi_0(\chi_0)+\psi_1(\chi_0,\chi_1)\cdot 2+\psi_2(\chi_0,\chi_1,\chi_2)\cdot 2^2+\cdots .$$

We refer to these Boolean functions $\psi_0, \psi_1, \psi_2, \ldots$ as coordinate functions of the T-function f.

If the T-functions are restricted to the set of all numbers whose base-2 expansions are not longer than k, we sometimes refer to these restrictions as T-functions on k-bit words: We usually associate the set of all k-bit words to the set $\{0, 1, \ldots, 2^k - 1\}$ of all residues modulo 2^k; the latter set constitutes the residue ring $\mathbb{Z}/2^k\mathbb{Z}$ modulo 2^k w.r.t. modulo 2^k operations of addition and multiplication.

T-functions are 2-adic maps

T-functions may be viewed as mappings from 2-adic integers to 2-adic integers: e.g., for a univariate T-function f

$$\chi_0+\chi_1\cdot 2+\chi_2\cdot 2^2+\cdots \stackrel{f}{\mapsto} \psi_0(\chi_0)+\psi_1(\chi_0,\chi_1)\cdot 2+\psi_2(\chi_0,\chi_1,\chi_2)\cdot 2^2+\cdots .$$

We refer to these Boolean functions $\psi_0, \psi_1, \psi_2, \ldots$ as coordinate functions of the T-function f.

If the T-functions are restricted to the set of all numbers whose base-2 expansions are not longer than k, we sometimes refer to these restrictions as T-functions on k-bit words: We usually associate the set of all k-bit words to the set $\{0, 1, \ldots, 2^k - 1\}$ of all residues modulo 2^k; the latter set constitutes the residue ring $\mathbb{Z}/2^k\mathbb{Z}$ modulo 2^k w.r.t. modulo 2^k operations of addition and multiplication.

T-functions are 2-adic maps

T-functions may be viewed as mappings from 2-adic integers to 2-adic integers: e.g., for a univariate T-function f

$$\chi_0+\chi_1\cdot 2+\chi_2\cdot 2^2+\cdots \stackrel{f}{\mapsto} \psi_0(\chi_0)+\psi_1(\chi_0,\chi_1)\cdot 2+\psi_2(\chi_0,\chi_1,\chi_2)\cdot 2^2+\cdots .$$

We refer to these Boolean functions $\psi_0, \psi_1, \psi_2, \ldots$ as coordinate functions of the T-function f.

If the T-functions are restricted to the set of all numbers whose base-2 expansions are not longer than k, we sometimes refer to these restrictions as T-functions on k-bit words: We usually associate the set of all k-bit words to the set $\{0, 1, \ldots, 2^k - 1\}$ of all residues modulo 2^k; the latter set constitutes the residue ring $\mathbb{Z}/2^k\mathbb{Z}$ modulo 2^k w.r.t. modulo 2^k operations of addition and multiplication.

T-functions are *continuous* 2-adic maps

The most important is that all T-functions are continuous functions of 2-adic variables since all T-functions satisfy a Lipschitz condition with a constant 1 with respect to the 2-adic metric, and vice versa.

1-Lipschtiz functions=Compatible functions=T-functions

A map $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ satisfies a 2-adic Lipschtiz condition with a constant 1 : $|f(a) - f(b)|_2 \le |a - b|_2$ for all $a, b \in \mathbb{Z}_2$ iff f is compatible: if $a \equiv b \pmod{2^k}$, then $f(a) \equiv f(b) \pmod{2^k}$. This is equivalent to the condition that f is a T-function.

The following functions satisfy the Lipschitz condition with a constant 1 and thus are T-functions (and so also be used in compositions of cryptographic primitives):

1. subtraction $(u, v) \mapsto u - v$;
2. exponentiation $(u, v) \mapsto (1 + 2u)^v$;
3. negative powers, $u \mapsto (1 + 2u)^{-n}$;
4. division $(u, v) \mapsto \frac{u}{1+2v}$.

T-functions are *continuous* 2-adic maps

The most important is that all T-functions are continuous functions of 2-adic variables since all T-functions satisfy a Lipschitz condition with a constant 1 with respect to the 2-adic metric, and vice versa.

1-Lipschtiz functions=Compatible functions=T-functions

A map $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ satisfies a 2-adic Lipschtiz condition with a constant $1 : |f(a) - f(b)|_2 \leq |a - b|_2$ for all $a, b \in \mathbb{Z}_2$ iff f is compatible: if $a \equiv b \pmod{2^k}$, then $f(a) \equiv f(b) \pmod{2^k}$. This is equivalent to the condition that f is a T-function.

The following functions satisfy the Lipschitz condition with a constant 1 and thus are T-functions (and so also be used in compositions of cryptographic primitives):

1. subtraction $(u, v) \mapsto u - v$;
2. exponentiation $(u, v) \mapsto (1 + 2u)^v$;
3. negative powers, $u \mapsto (1 + 2u)^{-n}$;
4. division $(u, v) \mapsto \frac{u}{1+2v}$.

T-functions are *continuous* 2-adic maps

The most important is that all T-functions are continuous functions of 2-adic variables since all T-functions satisfy a Lipschitz condition with a constant 1 with respect to the 2-adic metric, and vice versa.

1-Lipschtiz functions=Compatible functions=T-functions

A map $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ satisfies a 2-adic Lipschtiz condition with a constant $1 : |f(a) - f(b)|_2 \le |a - b|_2$ for all $a, b \in \mathbb{Z}_2$ iff f is compatible: if $a \equiv b \pmod{2^k}$, then $f(a) \equiv f(b) \pmod{2^k}$. This is equivalent to the condition that f is a T-function.

The following functions satisfy the Lipschitz condition with a constant 1 and thus are T-functions (and so also be used in compositions of cryptographic primitives):

1. subtraction $(u, v) \mapsto u - v$;
2. exponentiation $(u, v) \mapsto (1 + 2u)^v$;
3. negative powers, $u \mapsto (1 + 2u)^{-n}$;
4. division $(u, v) \mapsto \frac{u}{1+2v}$.

T-functions are *continuous* 2-adic maps

The most important is that all T-functions are continuous functions of 2-adic variables since all T-functions satisfy a Lipschitz condition with a constant 1 with respect to the 2-adic metric, and vice versa.

1-Lipschtiz functions=Compatible functions=T-functions

A map $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ satisfies a 2-adic Lipschtiz condition with a constant $1: |f(a) - f(b)|_2 \le |a - b|_2$ for all $a, b \in \mathbb{Z}_2$ iff f is compatible: if $a \equiv b \pmod{2^k}$, then $f(a) \equiv f(b) \pmod{2^k}$. This is equivalent to the condition that f is a T-function.

The following functions satisfy the Lipschitz condition with a constant 1 and thus are T-functions (and so also be used in compositions of cryptographic primitives):

1. subtraction $(u, v) \mapsto u - v$;
2. exponentiation $(u, v) \mapsto (1 + 2u)^v$;
3. negative powers, $u \mapsto (1 + 2u)^{-n}$;
4. division $(u, v) \mapsto \frac{u}{1+2v}$.

T-functions are *continuous* 2-adic maps

The most important is that all T-functions are continuous functions of 2-adic variables since all T-functions satisfy a Lipschitz condition with a constant 1 with respect to the 2-adic metric, and vice versa.

1-Lipschtiz functions=Compatible functions=T-functions

A map $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ satisfies a 2-adic Lipschtiz condition with a constant $1 : |f(a) - f(b)|_2 \le |a - b|_2$ for all $a, b \in \mathbb{Z}_2$ iff f is compatible: if $a \equiv b \pmod{2^k}$, then $f(a) \equiv f(b) \pmod{2^k}$. This is equivalent to the condition that f is a T-function.

The following functions satisfy the Lipschitz condition with a constant 1 and thus are T-functions (and so also be used in compositions of cryptographic primitives):

1. subtraction $(u, v) \mapsto u - v$;
2. exponentiation $(u, v) \mapsto (1 + 2u)^v$;
3. negative powers, $u \mapsto (1 + 2u)^{-n}$;
4. division $(u, v) \mapsto \frac{u}{1+2v}$.

Derivations of T-functions

Derivations of T-functions are defined in the same way as in classical Calculus. Note that as a T-function is a 1-Lipschitz function w.r.t. 2-adic metric, *the derivative must be a 2-adic integer* (provided the derivative exists).

Definition 1 (uniform differentiability modulo 2^M)

Given $M \in \mathbb{N} = \{1, 2, 3, \ldots\}$, a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is called uniformly differentiable modulo 2^M iff there exists $K \in \mathbb{N}$ such that once $\|h\|_2 \leqslant \frac{1}{2^K}$ (that is, once $h \equiv 0 \pmod{2^K}$)*, for all $x \in \mathbb{Z}_2$, the congruence*

$$f(x+h) \equiv f(x) + f'_M(x) \cdot h \pmod{2^{ord_2 h + M}}$$

holds. The minimum $K = K(M)$ is denoted via $N_M(f)$.

Here $ord_2(h) = -\log_2 |h|_2$ is just the length of the longest 0-prefix in representation of h as an infinite binary word.

Derivations of T-functions

Derivations of T-functions are defined in the same way as in classical Calculus. Note that as a T-function is a 1-Lipschitz function w.r.t. 2-adic metric, *the derivative must be a 2-adic integer* (provided the derivative exists).

Definition 1 (uniform differentiability modulo 2^M)

Given $M \in \mathbb{N} = \{1, 2, 3, \ldots\}$, a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is called uniformly differentiable modulo 2^M iff there exists $K \in \mathbb{N}$ such that once $\|h\|_2 \leqslant \frac{1}{2^K}$ (that is, once $h \equiv 0 \pmod{2^K}$)*, for all $x \in \mathbb{Z}_2$, the congruence*

$$f(x+h) \equiv f(x) + f'_M(x) \cdot h \pmod{2^{ord_2 h + M}}$$

holds. The minimum $K = K(M)$ is denoted via $N_M(f)$.

Here $ord_2(h) = -\log_2 |h|_2$ is just the length of the longest 0-prefix in representation of h as an infinite binary word.

Classes of differentiability

- From the definition of uniform differentiability modulo 2^M it readily follows that the derivative modulo 2^M is defined up to a summand which is 0 modulo 2^M. Furthermore, it can be proved that a derivative modulo 2^M is a periodic function with a period of length $2^{N_M(f)}$.
- It is obvious that if a T-function is uniformly differentiable modulo 2^{M+1} then it is uniformly differentiable modulo 2^M. So, we have a hierarchy of classes of uniform differentiability,

$$\mathfrak{D}_1 \supset \mathfrak{D}_2 \supset \mathfrak{D}_3 \supset \cdots \supset \mathfrak{D}_\infty,$$

where $\mathfrak{D}_i$ is the class of all T-functions that are uniformly differentiable modulo 2^i, and $\mathfrak{D}_\infty$ is a class of all uniformly differentiable T-functions. It turns out that *the T-functions of major interest to cryptography, the invertible ones, all lie in $\mathfrak{D}_1$; i.e., they all are uniformly differentiable modulo 2.*

Classes of differentiability

- From the definition of uniform differentiability modulo 2^M it readily follows that the derivative modulo 2^M is defined up to a summand which is 0 modulo 2^M. Furthermore, it can be proved that a derivative modulo 2^M is a periodic function with a period of length $2^{N_M(f)}$.
- It is obvious that if a T-function is uniformly differentiable modulo 2^{M+1} then it is uniformly differentiable modulo 2^M. So, we have a hierarchy of classes of uniform differentiability,

$$\mathfrak{D}_1 \supset \mathfrak{D}_2 \supset \mathfrak{D}_3 \supset \cdots \supset \mathfrak{D}_\infty,$$

where $\mathfrak{D}_i$ is the class of all T-functions that are uniformly differentiable modulo 2^i, and $\mathfrak{D}_\infty$ is a class of all uniformly differentiable T-functions. It turns out that *the T-functions of major interest to cryptography, the invertible ones, all lie in $\mathfrak{D}_1$; i.e., they all are uniformly differentiable modulo 2.*

Classes of differentiability

- From the definition of uniform differentiability modulo 2^M it readily follows that the derivative modulo 2^M is defined up to a summand which is 0 modulo 2^M. Furthermore, it can be proved that a derivative modulo 2^M is a periodic function with a period of length $2^{N_M(f)}$.
- It is obvious that if a T-function is uniformly differentiable modulo 2^{M+1} then it is uniformly differentiable modulo 2^M. So, we have a hierarchy of classes of uniform differentiability,

$$\mathfrak{D}_1 \supset \mathfrak{D}_2 \supset \mathfrak{D}_3 \supset \cdots \supset \mathfrak{D}_\infty,$$

where $\mathfrak{D}_i$ is the class of all T-functions that are uniformly differentiable modulo 2^i, and $\mathfrak{D}_\infty$ is a class of all uniformly differentiable T-functions. It turns out that *the T-functions of major interest to cryptography, the invertible ones, all lie in $\mathfrak{D}_1$; i.e., they all are uniformly differentiable modulo 2*.

Bijectivity and transitivity modulo 2^n and on $\mathbb{Z}_2$

The compatibility implies that given a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ and $n \in \mathbb{N} = \{1, 2, 3, \ldots\}$, the map $f \bmod 2^n\colon z \mapsto f(z) \bmod 2^n$ is a well-defined transformation of the residue ring $\mathbb{Z}/2^n\mathbb{Z} = \{0, 1, \ldots, 2^n - 1\}$; actually the reduced map $f \bmod 2^n$ is a T-function on n-bit words.

- Given $n \in \mathbb{N}$, a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is said to be bijective (resp., transitive) modulo 2^n iff it is invertible (resp. transitive) on n-bit words; that is, iff the reduced map $f \bmod 2^n\colon \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{Z}/2^n\mathbb{Z}$ is a permutation (resp., a permutation with the only cycle, of length 2^n) on the residue ring $\mathbb{Z}/2^n\mathbb{Z}$

Definition 2 (Bijectivity, transitivity)

We say that a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is bijective iff it is bijective modulo 2^n for all $n \in \mathbb{N}$; we say that f is transitive iff f is transitive modulo 2^n for all $n \in \mathbb{N}$.

Actually the definition is a theorem that is proved in the p-adic ergodic theory.

Bijectivity and transitivity modulo 2^n and on $\mathbb{Z}_2$

The compatibility implies that given a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ and $n \in \mathbb{N} = \{1,2,3,\ldots\}$, the map $f \bmod 2^n\colon z \mapsto f(z) \bmod 2^n$ is a well-defined transformation of the residue ring $\mathbb{Z}/2^n\mathbb{Z} = \{0,1,\ldots,2^n-1\}$; actually the reduced map $f \bmod 2^n$ is a T-function on n-bit words.

- Given $n \in \mathbb{N}$, a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is said to be bijective (resp., transitive) modulo 2^n iff it is invertible (resp. transitive) on n-bit words; that is, iff the reduced map $f \bmod 2^n\colon \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{Z}/2^n\mathbb{Z}$ is a permutation (resp., a permutation with the only cycle, of length 2^n) on the residue ring $\mathbb{Z}/2^n\mathbb{Z}$

Definition 2 (Bijectivity, transitivity)

We say that a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is bijective iff it is bijective modulo 2^n for all $n \in \mathbb{N}$; we say that f is transitive iff f is transitive modulo 2^n for all $n \in \mathbb{N}$.

Actually the definition is a theorem that is proved in the p-adic ergodic theory.

Bijectivity and transitivity modulo 2^n and on $\mathbb{Z}_2$

The compatibility implies that given a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ and $n \in \mathbb{N} = \{1, 2, 3, \ldots\}$, the map $f \bmod 2^n\colon z \mapsto f(z) \bmod 2^n$ is a well-defined transformation of the residue ring $\mathbb{Z}/2^n\mathbb{Z} = \{0, 1, \ldots, 2^n - 1\}$; actually the reduced map $f \bmod 2^n$ is a T-function on n-bit words.

- Given $n \in \mathbb{N}$, a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is said to be bijective (resp., transitive) modulo 2^n iff it is invertible (resp. transitive) on n-bit words; that is, iff the reduced map $f \bmod 2^n\colon \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{Z}/2^n\mathbb{Z}$ is a permutation (resp., a permutation with the only cycle, of length 2^n) on the residue ring $\mathbb{Z}/2^n\mathbb{Z}$

Definition 2 (Bijectivity, transitivity)

We say that a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is bijective iff it is bijective modulo 2^n for all $n \in \mathbb{N}$; we say that f is transitive iff f is transitive modulo 2^n for all $n \in \mathbb{N}$.

Actually the definition is a theorem that is proved in the p-adic ergodic theory.

Bijectivity and transitivity of differentiable T-functions

In the p-adic ergodic theory the following assertions are proved:

Theorem 3 (Bijectivity/transitivity conditions)

- *If a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is bijective then it is uniformly differentiable modulo 2 and its derivative modulo 2 is 1 everywhere: $f_1'(x) \equiv 1 \pmod 2$ for all $x \in \mathbb{Z}_2$* (equivalently, for all $x \in \mathbb{Z}/2^{N_1(f)}\mathbb{Z}$).
- *Let a T-function f be uniformly differentiable modulo 2. Then f is bijective iff f is bijective modulo $2^{N_1(f)}$ and $f_1'(x) \equiv 1 \pmod 2$ everywhere. Equivalently: if and only if f is bijective modulo $2^{N_1(f)+1}$.*
- *Let a T-function f be uniformly differentiable modulo 4. Then f is transitive iff f is transitive modulo $2^{N_2(f)+2}$.*

For instance, the Klimov-Shamir T-function $f(x) = x + (x^2 \vee 5)$ is transitive since f is uniformly differentiable, $N_2(f) = 2$; so it suffices to check whether the residues modulo 16 of $0, f(0), f^2(0) = f(f(0)), \ldots, f^{15}(0)$ are all different. This can readily be verified by direct calculations.

Bijectivity and transitivity of differentiable T-functions

In the p-adic ergodic theory the following assertions are proved:

Theorem 3 (Bijectivity/transitivity conditions)

- *If a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is bijective then it is uniformly differentiable modulo 2 and its derivative modulo 2 is 1 everywhere: $f'_1(x) \equiv 1 \pmod 2$ for all $x \in \mathbb{Z}_2$* (equivalently, for all $x \in \mathbb{Z}/2^{N_1(f)}\mathbb{Z}$).
- *Let a T-function f be uniformly differentiable modulo 2. Then f is bijective iff f is bijective modulo $2^{N_1(f)}$ and $f'_1(x) \equiv 1 \pmod 2$ everywhere. Equivalently: if and only if f is bijective modulo $2^{N_1(f)+1}$.*
- *Let a T-function f be uniformly differentiable modulo 4. Then f is transitive iff f is transitive modulo $2^{N_2(f)+2}$.*

For instance, the Klimov-Shamir T-function $f(x) = x + (x^2 \vee 5)$ is transitive since f is uniformly differentiable, $N_2(f) = 2$; so it suffices to check whether the residues modulo 16 of $0, f(0), f^2(0) = f(f(0)), \ldots, f^{15}(0)$ are all different. This can readily be verified by direct calculations.

Bijectivity and transitivity of differentiable T-functions

In the p-adic ergodic theory the following assertions are proved:

Theorem 3 (Bijectivity/transitivity conditions)

- *If a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is bijective then it is uniformly differentiable modulo 2 and its derivative modulo 2 is 1 everywhere: $f_1'(x) \equiv 1 \pmod 2$ for all $x \in \mathbb{Z}_2$* (equivalently, for all $x \in \mathbb{Z}/2^{N_1(f)}\mathbb{Z}$).
- *Let a T-function f be uniformly differentiable modulo 2. Then f is bijective iff f is bijective modulo $2^{N_1(f)}$ and $f_1'(x) \equiv 1 \pmod 2$ everywhere. Equivalently: if and only if f is bijective modulo $2^{N_1(f)+1}$.*
- *Let a T-function f be uniformly differentiable modulo 4. Then f is transitive iff f is transitive modulo $2^{N_2(f)+2}$.*

For instance, the Klimov-Shamir T-function $f(x) = x + (x^2 \vee 5)$ is transitive since f is uniformly differentiable, $N_2(f) = 2$; so it suffices to check whether the residues modulo 16 of $0, f(0), f^2(0) = f(f(0)), \ldots, f^{15}(0)$ are all different. This can readily be verified by direct calculations.

Bijectivity and transitivity of differentiable T-functions

In the p-adic ergodic theory the following assertions are proved:

Theorem 3 (Bijectivity/transitivity conditions)

- *If a T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ is bijective then it is uniformly differentiable modulo 2 and its derivative modulo 2 is 1 everywhere: $f_1'(x) \equiv 1 \pmod 2$ for all $x \in \mathbb{Z}_2$* (equivalently, for all $x \in \mathbb{Z}/2^{N_1(f)}\mathbb{Z}$).
- *Let a T-function f be uniformly differentiable modulo 2. Then f is bijective iff f is bijective modulo $2^{N_1(f)}$ and $f_1'(x) \equiv 1 \pmod 2$ everywhere. Equivalently: if and only if f is bijective modulo $2^{N_1(f)+1}$.*
- *Let a T-function f be uniformly differentiable modulo 4. Then f is transitive iff f is transitive modulo $2^{N_2(f)+2}$.*

For instance, the Klimov-Shamir T-function $f(x) = x + (x^2 \vee 5)$ is transitive since f is uniformly differentiable, $N_2(f) = 2$; so it suffices to check whether the residues modulo 16 of $0, f(0), f^2(0) = f(f(0)), \dots, f^{15}(0)$ are all different. This can readily be verified by direct calculations.

Properties of coordinate sequences

Given a transitive T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ and a 2-adic integer $x_0 \in \mathbb{Z}_2$, consider the *i-th coordinate sequence* $(\delta_i(f^j(x_0)))_{j=0}^{\infty}$.

- The sequence satisfies recurrence relation $\delta_i(x_{j+2^i}) \equiv \delta_i(x_j)+1 \pmod 2$, $0, 1, 2, \ldots$; that is, the second half of the period of the i-th coordinate sequence is bitwise negation of the first half;
- So the shortest period (which is of length 2^{i+1}) of the sequence is completely determined by its first 2^i bits.

Given *arbitrary* T-function f, the first half's of periods of coordinate sequences should be considered as independent, in the following meaning:

Theorem 4 (the independence of coordinate sequences)

Given a set $\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_2, \ldots$ of binary sequences $\mathcal{S}_i = (\zeta_j)_{j=0}^{2^i-1}$ of length 2^i, $i = 0, 1, 2, \ldots$, there exists a transitive T-function f and a 2-adic integer $x_0 \in \mathbb{Z}_2$ such that each first half of each i-th coordinate sequence is the sequence $\mathcal{S}_i$, $i = 0, 1, 2, \ldots$: $\delta_i(f^j(x_0)) = \zeta_j$, for all $j = 0, 1, \ldots, 2^i - 1$.

Properties of coordinate sequences

Given a transitive T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ and a 2-adic integer $x_0 \in \mathbb{Z}_2$, consider the *i-th coordinate sequence* $(\delta_i(f^j(x_0))_{j=0}^{\infty}$.

- The sequence satisfies recurrence relation $\delta_i(x_{j+2^i}) \equiv \delta_i(x_j)+1 \pmod 2$, $0, 1, 2, \ldots$; that is, the second half of the period of the i-th coordinate sequence is bitwise negation of the first half;
- So the shortest period (which is of length 2^{i+1}) of the sequence is completely determined by its first 2^i bits.

Given *arbitrary* T-function f, the first half's of periods of coordinate sequences should be considered as independent, in the following meaning:

Theorem 4 (the independence of coordinate sequences)

Given a set $\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_2, \ldots$ of binary sequences $\mathcal{S}_i = (\zeta_j)_{j=0}^{2^i-1}$ of length 2^i, $i = 0, 1, 2, \ldots$, there exists a transitive T-function f and a 2-adic integer $x_0 \in \mathbb{Z}_2$ such that each first half of each i-th coordinate sequence is the sequence $\mathcal{S}_i$, $i = 0, 1, 2, \ldots$: $\delta_i(f^j(x_0)) = \zeta_j, \quad$ for all $j = 0, 1, \ldots, 2^i - 1$.

Properties of coordinate sequences

Given a transitive T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ and a 2-adic integer $x_0 \in \mathbb{Z}_2$, consider the *i-th coordinate sequence* $(\delta_i(f^j(x_0))_{j=0}^{\infty}$.

- The sequence satisfies recurrence relation $\delta_i(x_{j+2^i}) \equiv \delta_i(x_j)+1 \pmod 2$, $0, 1, 2, \ldots$; that is, the second half of the period of the i-th coordinate sequence is bitwise negation of the first half;
- So the shortest period (which is of length 2^{i+1}) of the sequence is completely determined by its first 2^i bits.

Given *arbitrary* T-function f, the first half's of periods of coordinate sequences should be considered as independent, in the following meaning:

Theorem 4 (the independence of coordinate sequences)

Given a set $\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_2, \ldots$ of binary sequences $\mathcal{S}_i = (\zeta_j)_{j=0}^{2^i-1}$ of length 2^i, $i = 0, 1, 2, \ldots$, there exists a transitive T-function f and a 2-adic integer $x_0 \in \mathbb{Z}_2$ such that each first half of each i-th coordinate sequence is the sequence $\mathcal{S}_i$, $i = 0, 1, 2, \ldots$: $\delta_i(f^j(x_0)) = \zeta_j$, for all $j = 0, 1, \ldots, 2^i - 1$.

Properties of coordinate sequences

Given a transitive T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ and a 2-adic integer $x_0 \in \mathbb{Z}_2$, consider the *i-th coordinate sequence* $(\delta_i(f^j(x_0)))_{j=0}^{\infty}$.

- The sequence satisfies recurrence relation $\delta_i(x_{j+2^i}) \equiv \delta_i(x_j)+1 \pmod 2$, $0, 1, 2, \ldots$; that is, the second half of the period of the i-th coordinate sequence is bitwise negation of the first half;
- So the shortest period (which is of length 2^{i+1}) of the sequence is completely determined by its first 2^i bits.

Given *arbitrary* T-function f, the first half's of periods of coordinate sequences should be considered as independent, in the following meaning:

Theorem 4 (the independence of coordinate sequences)

Given a set $\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_2, \ldots$ of binary sequences $\mathcal{S}_i = (\zeta_j)_{j=0}^{2^i-1}$ of length 2^i, $i = 0, 1, 2, \ldots$, there exists a transitive T-function f and a 2-adic integer $x_0 \in \mathbb{Z}_2$ such that each first half of each i-th coordinate sequence is the sequence $\mathcal{S}_i$, $i = 0, 1, 2, \ldots$: $\delta_i(f^j(x_0)) = \zeta_j$, for all $j = 0, 1, \ldots, 2^i - 1$.

Properties of coordinate sequences

Given *arbitrary* T-function f, the first half's of periods of coordinate sequences should be considered as independent, in the following meaning:

Theorem 4 (the independence of coordinate sequences)

Given a set $\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_2, \ldots$ of binary sequences $\mathcal{S}_i = (\zeta_j)_{j=0}^{2^i-1}$ of length 2^i, $i = 0, 1, 2, \ldots$, there exists a transitive T-function f and a 2-adic integer $x_0 \in \mathbb{Z}_2$ such that each first half of each i-th coordinate sequence is the sequence $\mathcal{S}_i$, $i = 0, 1, 2, \ldots$: $\delta_i(f^j(x_0)) = \zeta_j, \quad$ for all $j = 0, 1, \ldots, 2^i - 1$.

The essence of our contribution:

If a transitive T-function is uniformly differentiable modulo 4 then its coordinate sequences can not be considered as independent: there are linear relations among them.

Linear dependencies

Given a transitive T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ and the initial state $x_0 \in \mathbb{Z}_2$, for $i = 0, 1, 2, \ldots$, $x_i = f^i(x_0)$, denote by $\chi_n^i = \delta_i(f^n(x_0))$ the n-th digit in the canonic 2-adic expansion of the n-th iterate of x_0. Our first result yields that if a transitive T-function is uniformly differentiable modulo 4 then *two* adjacent coordinate sequences satisfy a linear relation:

Linear dependencies

Given a transitive T-function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ and the initial state $x_0 \in \mathbb{Z}_2$, for $i = 0, 1, 2, \ldots$, $x_i = f^i(x_0)$, denote by $\chi_n^i = \delta_i(f^n(x_0))$ the n-th digit in the canonic 2-adic expansion of the n-th iterate of x_0. Our first result yields that if a transitive T-function is uniformly differentiable modulo 4 then *two* adjacent coordinate sequences satisfy a linear relation:

Theorem 5 (Linear relation between two adjacent coordinate sequences)

Let a transitive T-function f be uniformly differentiable modulo 4. Given $x_0 \in \mathbb{Z}_2$, for all $n \geq N_2(f) + 1$ the following congruence holds:

$$\chi_n^{i+2^{n-1}} \equiv \chi_{n-1}^i + \chi_n^i + \chi_{n-1}^0 + \chi_n^0 + \chi_n^{2^{n-1}} + y(i) \pmod 2. \tag{1}$$

The length of the shortest period of the binary sequence $(y(i))_{i=0}^{\infty}$ is 2^K, $0 \leq K \leq N_2(f)$. Furthermore, $y(i)$ does not depend on n.

Linear dependencies

Theorem 5 (Linear relation between two adjacent coordinate sequences)

Let a transitive T-function f be uniformly differentiable modulo 4. Given $x_0 \in \mathbb{Z}_2$, for all $n \geq N_2(f) + 1$ the following congruence holds:

$$\chi_n^{i+2^{n-1}} \equiv \chi_{n-1}^i + \chi_n^i + \chi_{n-1}^0 + \chi_n^0 + \chi_n^{2^{n-1}} + y(i) \pmod 2. \quad (1)$$

The length of the shortest period of the binary sequence $(y(i))_{i=0}^{\infty}$ is 2^K, $0 \leq K \leq N_2(f)$. Furthermore, $y(i)$ does not depend on n.

- Note that if a T-function is transitive then by Theorem 3 it is uniformly differentiable modulo 2; so conditions of the above theorem are not too restrictive: we only demand the T-function to lie in the second large differentiability class $\mathfrak{D}_2$.

Linear dependencies

Theorem 5 (Linear relation between two adjacent coordinate sequences)

Let a transitive T-function f be uniformly differentiable modulo 4. Given $x_0 \in \mathbb{Z}_2$, for all $n \geq N_2(f)+1$ the following congruence holds:

$$\chi_n^{i+2^{n-1}} \equiv \chi_{n-1}^{i} + \chi_n^{i} + \chi_{n-1}^{0} + \chi_n^{0} + \chi_n^{2^{n-1}} + y(i) \pmod 2. \quad (1)$$

The length of the shortest period of the binary sequence $(y(i))_{i=0}^{\infty}$ is 2^K, $0 \leq K \leq N_2(f)$. Furthermore, $y(i)$ does not depend on n.

- As both polynomial T-functions (the ones represented by polynomials over $\mathbb{Z}_2$) and the Klimov-Shamir T-function (of the form $x + (x^2 \vee C)$, $C \in \mathbb{Z}$) are uniformly differentiable (thus, lie in $\mathfrak{D}_\infty$ and whence in $\mathfrak{D}_2$), the above theorem could be considered as a generalization of results due to Wang and Qi, and to Molland and Helleseth.

Linear dependencies

Theorem 5 (Linear relation between two adjacent coordinate sequences)

Let a transitive T-function f be uniformly differentiable modulo 4. Given $x_0 \in \mathbb{Z}_2$, for all $n \geq N_2(f)+1$ the following congruence holds:

$$\chi_n^{i+2^{n-1}} \equiv \chi_{n-1}^{i} + \chi_n^{i} + \chi_{n-1}^{0} + \chi_n^{0} + \chi_n^{2^{n-1}} + y(i) \pmod 2. \qquad (1)$$

The length of the shortest period of the binary sequence $(y(i))_{i=0}^{\infty}$ is 2^K, $0 \leq K \leq N_2(f)$. Furthermore, $y(i)$ does not depend on n.

- The class of transitive T-functions that are uniformly differentiable modulo 4 is wide: for instance, it includes
  - all T-functions $f(x) = u(x) + 4 \cdot v(x)$ and $f(x) = u(x + 4 \cdot v(x))$, where u is a transitive T-function that is uniformly differentiable modulo 4 and v is an *arbitrary* T-function.

Linear dependencies

Theorem 5 (Linear relation between two adjacent coordinate sequences)

Let a transitive T-function f be uniformly differentiable modulo 4. Given $x_0 \in \mathbb{Z}_2$, for all $n \geq N_2(f) + 1$ the following congruence holds:

$$\chi_n^{i+2^{n-1}} \equiv \chi_{n-1}^{i} + \chi_n^{i} + \chi_{n-1}^{0} + \chi_n^{0} + \chi_n^{2^{n-1}} + y(i) \pmod 2. \tag{1}$$

The length of the shortest period of the binary sequence $(y(i))_{i=0}^{\infty}$ is 2^K, $0 \leq K \leq N_2(f)$. Furthermore, $y(i)$ does not depend on n.

- The class of transitive T-functions that are uniformly differentiable modulo 4 is wide: for instance, it includes
  - all T-functions of the form $f(x) = 1 + x + 2(g(x+1) - g(x))$ where g is a bijective T-function

Linear dependencies

Theorem 5 (Linear relation between two adjacent coordinate sequences)

Let a transitive T-function f be uniformly differentiable modulo 4. Given $x_0 \in \mathbb{Z}_2$, for all $n \geq N_2(f)+1$ the following congruence holds:

$$\chi_n^{i+2^{n-1}} \equiv \chi_{n-1}^i + \chi_n^i + \chi_{n-1}^0 + \chi_n^0 + \chi_n^{2^{n-1}} + y(i) \pmod 2. \quad (1)$$

The length of the shortest period of the binary sequence $(y(i))_{i=0}^{\infty}$ is 2^K, $0 \leq K \leq N_2(f)$. Furthermore, $y(i)$ does not depend on n.

- The class of transitive T-functions that are uniformly differentiable modulo 4 is wide: for instance, it includes
  - more specific functions, exponential functions of the form $f(x) = ax + a^x$, where $a \equiv 1 \pmod 2$; rational functions of the form $f(x) = \frac{u(x)}{1+4\cdot v(x)}$, where u is a transitive polynomial and v is arbitrary T-function.

Quadratic dependencies

Our second result yields that if a T-function lies in the third largest differentiability class $\mathfrak{D}_3$ then there exists a quadratic relation among *three* adjacent coordinate sequences:

Theorem 6 (Quadratic relation among three adjacent coordinate sequences)

Let a transitive T-function f be uniformly differentiable modulo 8. Given $x_0 \in \mathbb{Z}_2$, for all $n \geq N_3(f) + 2$ following congruence holds:

$$\chi_n^{i+2^{n-2}} \equiv \chi_{n-2}^i \chi_{n-1}^i + \theta(n,i)(\chi_{n-2}^i + \chi_{n-1}^i) + \chi_n^i + y_{n,i} \pmod 2, \qquad (2)$$

where $\theta(n,i) \in \{0,1\}$. Furthermore, the length of the shortest period of binary sequences $(\theta(n,i))_{i=0}^{\infty}$and $(y_{n,i})_{i=0}^{\infty}$ are factors of $2^{N_3(f)}$.

Theorem 6 may be considered as a generalization of a result of Luo and Qi, who proved quadratic relation for the Klimov-Shamir T-function.

Messages of the talk

<u>**Mathematics:**</u> We have proved that a vast body of transitive T-functions exhibit linear and quadratic weaknesses: we found a linear and a quadratic relation that are satisfied by output sequences generated by univariate transitive T-functions that constitute a very vast class $\mathfrak{D}_2$.

Earlier relations of this sort were known only for T-functions of two special types: for the Klimov-Shamir T-function $x + (x^2 \vee C)$ and for polynomials with integer coefficients. The class $\mathfrak{D}_2$ is much wider: it contains rational functions, exponential functions as well as their various compositions with bitwise logical operations.

Messages of the talk

Applications: On the base of methods we have developed, it can be proved that similar relations hold in output sequences of corresponding classes of *multivariate* T-functions as well as in output sequences of T-function-based counter-dependent generators; the latter are generators with a recursion law of the form $x_{i+1} = f_i(x_i)$.

Primitives of both types, the multivariate T-function-based ordinary generators and T-function-based counter-dependent generators, are used in stream ciphers, e.g., in ASC, TF-i, TSC, and in ABC. Therefore the relations we have found may be used to construct attacks against ciphers of this kind.

Thank you !