

# Cryptography midterm report

Tran Van Sang, Department of Computer Science, 48-186106  
Eguchi Shingo, Department of Computer Science, 48-186016

June 7, 2018

# Contents

<b>1</b>	<b>Topic</b>	<b>2</b>
<b>2</b>	<b>Hash function</b>	<b>3</b>
<b>3</b>	<b>ISBN</b>	<b>4</b>
3.1	Introduction . . . . .	4
3.2	Detection ability . . . . .	4
3.3	Proof . . . . .	5
3.3.1	Single digit modification . . . . .	5
3.3.2	Consecutive swapping . . . . .	5
3.3.3	Generalization . . . . .	5
<b>4</b>	<b>Credit card checksum</b>	<b>6</b>
<b>5</b>	<b>Dihedral Group</b>	<b>8</b>
<b>6</b>	<b>Quasigroup</b>	<b>9</b>
<b>7</b>	<b>Summary</b>	<b>10</b>

# Chapter 1

## Topic

We presented basic checksum algorithms such as the one used in credit card numbers. Explain what is a quasigroup. Present and analyze Dammm's method based on quasigroups to detect all single-digit and transposition errors. Are there other quasigroups that work ?

## Chapter 2

# Hash function

Hash function is a class of function that takes input of arbitrary length, called message, and outputs of fixed length, called hash. Hash function has important role in cryptography and many applications due to its one-wayness. Hash function ability to resist cryptanalytic attack is mainly determined by 3 properties

- Pre-image resistance. Sometime referred as one-wayness. Given a hash value  $h$ , it should be infeasible within acceptable time to find original domain value  $m$  such that the hash function maps  $m$  into  $h$ .
- Second pre-image resistance. It should be infeasible within acceptable time to find another input  $m'$  that has same image mapped by the hash function, given input  $m$ .
- Collision resistance. It should be infeasible within acceptable time to find 2 input messages  $m, m'$  such that the hash function maps them into same hash.

It is obvious that pre-image resistance hash function is also pre-image resistance. Similarly, functions that resist collision also have second pre-image resistance property.

## Chapter 3

# ISBN

### 3.1 Introduction

International Standard Book Number (ISBN) is an unique 13 digits long number assigned to a book. Affiliates of International ISBN Agency have ability to release a number whenever being requested by publisher. The last digit is the hash of 10 preceding digits. In other words,

$$\begin{aligned} ISBN &= m_{13}, m_{12}, m_{11}, \dots, m_1 \\ m_1 &= isbn(m_{13}, m_{12}, m_{11}, \dots, m_2) \end{aligned}$$

Whether

$$isbn(m_{13}, m_{12}, m_{11}, \dots, m_2) = \sum_{i \equiv 1 \pmod{2}, 2 \leq i \leq 13} m_i + 3 \times \sum_{i \equiv 0 \pmod{2}, 2 \leq i \leq 13} m_i$$

### 3.2 Detection ability

Using ISBN system, one can detect one digit changed or 2 consecutive digits swapped unless that those numbers' difference is 5 (i.e. swapping numbers are one of (0, 5), (1, 6), (2, 7), (3, 8), or (4, 9))

To check if there is any modification on the received ISBN number, one can check by calculating checksum  $C = \sum_{i \equiv 1 \pmod{2}, 2 \leq i \leq 13} m_i + 3 \times \sum_{i \equiv 0 \pmod{2}, 2 \leq i \leq 13} m_i - m_1 \pmod{10}$  equal to 0.

### 3.3 Proof

#### 3.3.1 Single digit modification

We will prove with this method 2 kinds of modification mentioned above can be detected.

Assume that  $i$ th number is changed to  $m'_i$  while other numbers keep the same. Absolute of difference between new sum and old sum is

$$|C - C'| \mod 10 = \begin{cases} |m_i - m'_i| \mod 10 & \text{if } i \equiv 1 \pmod{2} \\ 3 \times |m_i - m'_i| \mod 10 & \text{otherwise} \end{cases}$$

Because  $GCD(3, 10) = 1$ ,  $|C - C'| \mod 10 \neq 0$

#### 3.3.2 Consecutive swapping

If 2 digits  $m_i$  and  $m_{i+1}$  are swapped, and  $|m_i - m_{i+1}| \neq 5$   
Similar to previous subsection

$$\begin{aligned} |C - C'| \mod 10 &= \begin{cases} |m_i + 3 \times m_{i+1} - 3 \times m_i - m_{i+1}| \mod 10 & \text{if } i \equiv 1 \pmod{2} \\ |3 \times m_i + m_{i+1} - m_i - 3 \times m_{i+1}| \mod 10 & \text{otherwise} \end{cases} \\ &= 2 \times |m_i - m_{i+1}| \end{aligned} \tag{3.1}$$

Thus,  $|C - C'| \mod 10 \neq 0$

#### 3.3.3 Generalization

The ISBN checksum is one special case of the hash function  $H(m) = \sum_{i \geq 2} a_i m_i \mod 10$  where  $a_i (i \geq 2)$  are fixed

In the following chapter we will discuss on other form of checksum with better error detection ability.

## Chapter 4

# Credit card checksum

Credit card number contains  $n$  number  $m_n, m_{n-1}, \dots, m_2, m_1$  where  $n$  is variate depends on credit card provider. For example,  $n = 16$  for Visa, Master card,  $n = 19$  for UnionPay card

The following hash function is used in credit card to detect error

$$m_1 = H(m)$$

is chosen such that

$$\sum_{i \text{ is odd}} m_i + \sum_{i \text{ is even}} f(m_i) \equiv 0 \pmod{10}$$

whether

$$f(x) = 2x + \left\lfloor \frac{x}{5} \right\rfloor \pmod{10}$$

This  $f(x)$  is called Luhn (1954) function.

By this checksum, it is able to check for single digit error or consecutive digits swap unless they are not (0, 9) or (9, 0) pairs.

Before giving proof to the error resistance, we observe some properties of the Luhn function

x	0	1	2	3	4	5	6	7	8	9
f(x)	0	2	4	6	8	1	3	5	7	9
$(x - f(x)) \pmod{10}$	0	9	8	7	6	4	3	2	1	0

Firstly,  $f$  maps  $\{0, 1, \dots, 9\}$  to the same set  $\{0, 1, \dots, 9\}$  without collision. In other words, for all  $x_1 \neq x_2$   $f(x_1) \neq f(x_2)$ . Functions having this property are called permutation functions.

Secondly, there are only 2 fixed points (0 and 9), i.e.  $x = f(x)$  and for all  $x$ ,  $(x - f(x)) \pmod{10}$  are almost different except 0 and 9.

Now we move on proving the error resistance.

If only one digit is changed,  $m_i$  is changed to  $m'_i$ ,

$$|C - C'| \mod 10 = \begin{cases} |m_i - m'_i| \mod 10 & \text{if } i \equiv 1 \pmod{2} \\ f(m_i) - f(m'_i) \mod 10 & \text{otherwise} \end{cases}$$

Because of permutation property, this value never be zero. Thus, the error can be detected

If 2 consecutive number  $m_i, m_{i+1}$  are swapped.

$$\begin{aligned} |C - C'| \mod 10 &= \begin{cases} |m_i + f(m_{i+1}) - m_{i+1} - f(m_i)| \mod 10 & \text{if } i \equiv 1 \pmod{2} \\ |f(m_i) - m_{i+1} - f(m_{i+1}) - m_i| \mod 10 & \text{otherwise} \end{cases} \\ &= |(m_i - f(m_i) - (m_{i+1} - f(m_{i+1})))| \mod 10 \end{aligned} \quad (4.1)$$

If  $m_i = m_{i+1}$ , there is no need for detection. If  $m_i, m_{i+1}$  are not (0, 9) or (9, 0) pair, from the above table,  $m_i - f(m_i) \neq m_{i+1} - f(m_{i+1})$ . Thus,  $|C - C'| \mod 10 \neq 0$



## Chapter 5

# Dihedral Group

Content

# Chapter 6

## Quasigroup

Content

# Chapter 7

## Summary

Content