라이프 게임(세포자동자)을 이용한 암호화 알고리즘

AUTOMATA Hash Algorithm (AHA)

Team. AUTOMATA

김도현(長), 이재민, 손승재, 이경래, 최대원

최종수정: 2018.08.08.

- 개요

세포자동자를 이용하여 새로운 해시함수를 만든다.

- 상세

세포 자동자의 일종인 라이프 게임은 초기 상태가 주어지면 특정한 규칙에 따라 다음 단계의 모습이 결정된다. 그런데 초기 상태에서 다음 단계로 갈수록 예측하기 어려운 방식으로 변화한다. 나는 이러한 형태가 다음 단계를 예측하기 어렵다는 점을 이용하여, 이를 이용한 암호화 알고리즘을 고안해 보았다.

라이프 게임에서 입력값은 초기 상태(inmap[][])와 반복 횟수(N)이다. 그리고 결과값은 N회 반복한 상태(outmap[][])이다. 초기 상태와 결과값은 각각 2차원 좌표상의 점으로 나타난다.

평문을 세포 자동자의 초기값으로 인코딩한다. 그후 일정 횟수만큼 반복한 뒤에 나온 결과값을 암호문으로 저장한다. 이때 반복횟수는 공개(혹은 저장)한다.

- 문제점 및 해결법

1) 규칙변형 - **Before&After 시각 자료**

기존의 라이프게임 룰(23/3)을 이용한 경우 금방 수렴하거나, 다음 단계를 예측하기 쉬워 보안성이 약했다. 룰을 변형하여 쉽게 수렴되지 않고 예측이 어렵도록 보안성을 강화하였다.

특정 상태에 수렴하거나 규칙성을 가져 예측할 수 있는 경우를 대비하여 규칙을 변형한다.

2) 토러스형 격자 – **실제 종이를 이용하여 설명함**

입력값이나 실행횟수가 달라지면 출력값의 크기가 크게 변하는 문제를 발견하였다. 가장자리를 연결한 토러스 모양을 이용하면 해결할 수 있다.

3) 눈사태 효과 및 salt, MASK

6비트를 문자, 나머지 2비트를 MASK로 지정하여 salt 첨가, 눈사태 효과 증대

*\*문제상황을 그림으로 보여주기(전에는 어땠는데, 고친뒤에는 어떠하다), 그게 왜 문제가 되는지 설명하기!*

- 해야 할 것 **(최대한 쉽게 이해!)**

해시함수 설명 - **연극으로 설명**

결과값 크기, 걸리는 시간 등이 왜 중요한가

세포자동자는 무엇이며 어떤 의미인가 - **영상 중심으로**

규칙 변형하기 전 여러 수렴값을 보여준 뒤 "기존의 룰을 사용했을 때 수렴하는 모양이 비슷하여 룰을 변경하였다" 라고 말하고 변형한 뒤의 격자 보여주기

- 규칙 변형의 예

[태어나기(B)/생존하기(S)], 기본규칙은 (3,23), 앱의 순서와 동일, 위키피디아와 반대

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 규칙명 | 수렴 저항성 | 규칙 저항성(x4) | 개체수 편차(x3) | 평균 근방 (x1) | 점수 합계 |
| Gnarl (1/1) | O | 3 | 3 | 1 | 22 |
| 1237/157 | O | 3 | 3 | 3 | 24 |
| 1357/57 | O | 2 | 3 | 3 | 20 |
| 16/24 | O | 2 | 1 | 1 | 12 |
| 2/2 | O | 1 | 3 | 1 | 14 |
| 2/23 | X | 1 |  |  | 망 |
| 2/3 | X | 1 |  |  | 망 |
| 2/4 | O | 2 | 1 | 1 | 12 |
| 2/12 | O | 2 | 3 | 2 | 19 |
| 2/235 | X | 1 |  |  | 망 |

- 순서도 **(II.1. 탐구과정)** (웹사이트에 활용되는 상황)

가. 해시함수 생성 (함수 지정)

1) 인코딩 테이블 지정

2) 반복횟수 지정

3) salt 설정

나. 해시값 생성 (회원가입)

1) 입력값 인코딩 (문자->2진수)

2) AHA실행

3) 결과값 디코딩 (2진수->문자)

4) 해시값 서버에 저장

다. 해시값 비교 (로그인)

1) 나.1) ~ 4) 과정 실행

2) 결과값과 서버에 저장된 해시값 비교

- 참고자료

http://terms.naver.com/entry.nhn?docId=3534072&cid=58541&categoryId=58541 - 지식백과 라이프게임

**<목차>**

I. 서론

I.1. 참여자 목록 및 역할

I.2. 탐구 동기 및 목적

I.3. 이론적 배경

I.3.1. 세포자동자

I.3.2. 콘웨이의 라이프 게임

I.3.3. 단방향 암호 알고리즘과 해시함수 ***(보안의 3요소)***

II. 본론

II.1. 탐구과정 **(순서도)**

II.1.1. 해시함수 생성

II.1.2. 해시값 생성

II.1.3. 해시값 비교

II.2. 문제점

II.2.1. 결과값 크기 변동

II.2.2. 수렴문제

II.2.3. 보안성 의문 (레인보우 테이블 공격 방어)

II.3. 문제 해결 방법 ***(해결 전 후 비교해서 얻은 효과 보여주기)***

II.3.1. 토러스형 격자

II.3.2. 규칙 변형

II.3.3. 눈사태 효과 *(salt MASK 효과)*

III. 결론

III.1. 탐구 결과 분석

III.2. 탐구의 의의 및 한계 *(우리 것 자랑)*

III.3. AHA의 활용방안

IV. 참고문헌

**김도현, 이재민, 손승재, 이경래, 최대원**

**<Incoding Table>**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 10진수 | 2진수 | 16진수 | 문자 | 10진수 | 2진수 | 16진수 | 문자 |
| 0 | 00 0000 | 00 | ~ | 32 | 10 0000 | 20 | u |
| 1 | 00 0001 | 01 | ! | 33 | 10 0001 | 21 | v |
| 2 | 00 0010 | 02 | @ | 34 | 10 0010 | 22 | w |
| 3 | 00 0011 | 03 | # | 35 | 10 0011 | 23 | x |
| 4 | 00 0100 | 04 | $ | 36 | 10 0100 | 24 | y |
| 5 | 00 0101 | 05 | % | 37 | 10 0101 | 25 | z |
| 6 | 00 0110 | 06 | ^ | 38 | 10 0110 | 26 | A |
| 7 | 00 0111 | 07 | & | 39 | 10 0111 | 27 | B |
| 8 | 00 1000 | 08 | \* | 40 | 10 1000 | 28 | C |
| 9 | 00 1001 | 09 | \_ | 41 | 10 1001 | 29 | D |
| 10 | 00 1010 | 0A | + | 42 | 10 1010 | 2A | E |
| 11 | 00 1011 | 0B | | | 43 | 10 1011 | 2B | F |
| 12 | 00 1100 | 0C | a | 44 | 10 1100 | 2C | G |
| 13 | 00 1101 | 0D | b | 45 | 10 1101 | 2D | H |
| 14 | 00 1110 | 0E | c | 46 | 10 1110 | 2E | I |
| 15 | 00 1111 | 0F | d | 47 | 10 1111 | 2F | J |
| 16 | 01 0000 | 10 | e | 48 | 11 0000 | 30 | K |
| 17 | 01 0001 | 11 | f | 49 | 11 0001 | 31 | L |
| 18 | 01 0010 | 12 | g | 50 | 11 0010 | 32 | M |
| 19 | 01 0011 | 13 | h | 51 | 11 0011 | 33 | N |
| 20 | 01 0100 | 14 | i | 52 | 11 0100 | 34 | O |
| 21 | 01 0101 | 15 | j | 53 | 11 0101 | 35 | P |
| 22 | 01 0110 | 16 | k | 54 | 11 0110 | 36 | Q |
| 23 | 01 0111 | 17 | l | 55 | 11 0111 | 37 | R |
| 24 | 01 1000 | 18 | m | 56 | 11 1000 | 38 | S |
| 25 | 01 1001 | 19 | n | 57 | 11 1001 | 39 | T |
| 26 | 01 1010 | 1A | o | 58 | 11 1010 | 3A | U |
| 27 | 01 1011 | 1B | p | 59 | 11 1011 | 3B | V |
| 28 | 01 1100 | 1C | q | 60 | 11 1100 | 3C | W |
| 29 | 01 1101 | 1D | r | 61 | 11 1101 | 3D | X |
| 30 | 01 1110 | 1E | s | 62 | 11 1110 | 3E | Y |
| 31 | 01 1111 | 1F | t | 63 | 11 1111 | 3F | Z |

**<To Do List>**

**-해시함수란 (개념과 사례)**

**-세포자동자란 (그림 중심)**

**-라이프게임이란 (그림 중심)**

**라이프게임을 이용한 해시함수 설명 (순서도 내용 넣기, 구체적으로)**

**기존 해시함수와 AHA해시함수 비교 (연산속도, 충돌가능성, 눈덩이효과)**

**정보보안의 3요소 - 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)**

**이론적 배경에 넣으면 좋을 내용, 모르는 사람이 이해하기 위해 알아야 할 배경지식에 무엇이 있을지 대원이한테 물어서 넣기**

**III.1. 탐구결과분석 (문제점 해결하여 좋아진 점)**

***1. 조금만 바뀌어도 많이 변하는가?***

***2. 반복하면 못알아보게 바뀌는가?***

***3. 기존의 알고리즘과 비교, 분석 (결과동일성, 보안성, 눈사태 효과 등, 충돌저항성과 연산속도는 어쩔 수 없이 빼자)***

**III.2. 의의 (장점)**

***세포자동자의 예측 불가능한 성질을 암호에 적용하였다는 발상이 참신함***

***바로 실전에 적용할 만큼 보안성이 뛰어남***

***-어려운 수학적 배경지식이 없더라도 안전한 해시함수를 만들 수 있음***

***양자컴퓨터에 대비 가능***

**분량은 어느정도 되어야 하지? 올해 대회 담당하시는 선생님들은 누구지? 배경지식 설명시간 추가로 받을 수 있을까?**

**Q. 처음에 제기한 문제(네이트 해킹)를 AHA로 어떻게 개선했는가?**

**A. 네이트가 쓰던 해시함수는 MD5로, 이는 설계상의 허점이 발견되었다. MD5는 AHA보다 훨씬 복잡한 수학적 성질을 이용하기 때문에, 쉽게 취약점이 드러나지 않았지만, AHA는 수학적 성질을 이용하지 않고 세포자동자의 무질서한 성질을 이용하기 때문에 취약점을 쉽게 개선할 수 있다.**

**6bit(input) + 2bit(salt)로 바꾸기 (대소문자 52자+특수문자 12자)**

**자랑1. 원래 해시함수는 같은 input에 대하여 같은 output이 나와서 미리 hashing 해둔 값이랑 비교했을 때 간단한 password의 경우 금방 풀림, 하지만 salt를 두어 같은 input이라도 salt에 따라 값을 달리 할 수 있음 -> 레인보우테이블 공격 기법에 대응 (사실 salt의 장점에 해당됨, 우리만의 자랑이 아님)**

**Q. 기존의 해시함수와 비교했을 때 AHA는 어떤 점이 좋은가? 또는 정말로 좋은가?**

**A. 사실 보안이라는 것은 용도에 따라 다양한 성능, 기능이 존재한다. 우리의 AHA는 기존의 알고리즘보다는 느릴지 모르지만 뛰어난 보안성을 지니고 있어 고수준의 보안성이 필요한 곳에 쓰일 것이다.**

**- 처음에 암호관련 학술을 하고 싶어서 해시함수를 만들기로 하였는데 기존의 방식은 너무 복잡하고 어려워 시도하기가 어려웠다. 그러던 도중 세포자동자라는 개념을 알게 되고, 이것이 간단한 규칙으로 복잡한 단계를 생성한다는 특징이 해시함수와 적합하다고 생각하여 이를 해시함수에 이용해보기로 하였다.**

**(단순히 해시함수와 세포자동자를 결합한 것이 아닌, 해시함수를 하려고 하다가 세포자동자를 발견하여 이를 더한 것, 순차적으로)**

**- 우리가 하려는 것은 연구가 아닌 탐구다. 따라서 결과를 내는 것이 중요한 "연구"가 아닌 알아내는 과정이 중요한 "탐구"이다. 따라서 우리의 과정이 더욱 중요함**

**- 작년 아쿠아포닉스 팀은 화학적인 내용을 발표에 담지 않았다. 우리도 수학적인 원리는 줄이고 중요한 내용을 더욱 부각하는것이 좋을듯**

**- 수상팀 모두 뭔가 노가다같은 활동이 있다.**

**재민:**

**- 사례중심으로 소개 -> 이해가 쉽도록, 미리 자료배포해서 이해 도움, 세포자동자보다는 해시함수에 중점**

**- 우리가 성과를 이루었다고 자랑하는것보단, 우리들의 성장에 중점을 맞춤 (작년 수상팀처럼)**

**- 성공한 가설도 중요하지만 실패한 것도 아주 중요하다.**

**- 작년 수상팀을 분석했을 때 논문으로서의 질은 떨어진다. 하지만 자신들의 예측과 다른 새로운 점을 발견하여 가설을 수정하고, 새로운 사실을 알아내었다는 점이 좋게 평가됨.**

**- 사실 우리가 배꼈는지 실제로 한건지 알 방법이 없음.**

**<도서 구매 목록>**

**박경미의 수학콘서트 플러스(박경미, 동아시아)**

**전체 크기: 32x24, 솔트 크기 32자, 원문 크기 96자**