Diffie-Hellman Key Exchange を通して学ぶ Hardness Assumptions

暗号理論輪読会(2023/5/22)

speed

Agenda

- 群論入門
- Diffie-Hellman Key Exchange を通して学ぶ Hardness Assumptions
  - Diffie-Hellman Key Exchange
  - Discrete Log Assumption (DL仮定)
  - Computational Diffie-Hellman Assumption (CDH仮定)
  - Diffie-Hellman Key Exchangeの注意: Man In the Middle Attack(MITM)
- その他の重要なAssumptions
  - RSA Assumption(RSA仮定)
  - Learning with Errors (LWE)
  - 余談: 耐量子暗号としての格子暗号

群論入門

Definition: 群

> Gを空集合ではない集合とする. G上の2項演算$* : G \times G \to G$が定義されていて次の性質を満たすとき, $(G, *)$を群という.
>
> 1. 単位元の存在: 単位元と呼ばれる元$e \in G$が存在し, 任意の$a \in G$に対し, $a * e = e * a = a$となる.
> 2. 逆元の存在: 任意の$a \in G$に対し$b \in G$が存在し, $a * b = b * a = e$となる. bはaの逆元と呼ばれ, a^{-1}と書く.
> 3. 結合法則: すべての$a, b, c \in G$に対し, $(a * b) * c = a * (b * c)$が成り立つ.

群の例

- $(Z, +) = \{\dots, -2, -1, 0, 1, 2, \dots\}, (Z/3Z, +) = \{\bar{0}, \bar{1}, \bar{2}\}, (R\backslash\{0\}, *)$

群でない例

- $(Z\backslash\{0\}, *)$(逆元の存在が成り立たない, $2^{-1} \notin Z$)

Definition: 群Gの位数

群Gの要素数$\left|G\right|$をGの位数と呼ぶ

例

- $Z/pZ = \{0, 1, . . , p - 1\}$の位数は$p$
- Zの位数は∞

Definition: 可換群(Abelian Group)

> 可換群Gは, 群Gであって以下の性質を満たすもの
>
> - 交換法則: 任意の$a, b \in G$ に対して, $ab = ba$が成り立つ.

可換群の例

- $(Z, +)$: 4 + 5 = 5 + 4

可換群でない例

- $(n次正則行列全体の集合, *)$: $AB \neq BA$

Definition: 冪乗

$a \in G, n \in Z$に対して, $n \in N$に対し, a^nを次のように定義する.

> $a^0 = e$
> $a^{n+1} = a^n * a$
> $a^{-n} = (a^{-1})^n$

注意

- 群の定義のみでは冪乗という演算が定められていないため, 定義してやる必要がある.
- 加法群では$a * n = a + a + \ldots + a$のように表すこともある.

Definition: 巡回群

> 群Gが巡回群であるとは, ある元$g \in G$ が存在し, 任意の元$x \in G$ が $x = g^n (n \in Z)$ で表せるということ. (この時Gを$< g >$で表すことがある)

つまり, ある一つの元gの冪乗でGの全ての元を表せるということ.

> gは生成元と呼ばれる.

巡回群の例

- $g^n = 1$なるgにたいし, $G = \{1, g, g^1, g^2, \ldots, g^{n-1}\}$
- Z = <1> = {-2=(-1)+(-1), -1, 0={1}^0, 1, 2=1+1, 3=1+1+1,..}. Zは位数が無限の巡回群
- Z/pZ = {0, 1, 2, ..., p-1}は位数がpの巡回群

Definition: 元の位数

> 群Gの元xに対して, $x^n = e$ となる最小の正の整数nをxの位数と呼ぶ.

注意

群Gの位数はGの要素の数を表す. 元の位数はそれとは別物.

例

- Z/3Z = {0, 1, 2}の位数は|Z/3Z|=3より3.
- 一方, 1$\in Z/3Z$の位数は1. 2$\in Z/3Z$)の位数は2($\because 2^2 = 1 \bmod 3$)

Diffie-Hellman Key Exchange を通して学ぶ Hardness Assumptions

Diffie-Hellman Key Exchange(DH Key Exchange)

DH Key Exchangeの背景

- 鍵配送問題
  共通鍵で安全に情報をやり取りできたとして, 共通鍵をどのように攻撃者にバレないようにして通信相手と共有する?

DH Key Exchange の仕組み

1. 整数g, pをAliceとBobが共有
2. Aliceは秘密鍵a, Bobは秘密鍵bをそれぞれ持つ
3. Aliceは公開鍵$K_A = g^a \mod p$, Bobは公開鍵$K_B = g^b \mod p$を公開
4. AliceはBobの公開鍵を用いて$(K_B)^a = g^{ab} \mod p$を計算
5. BobはAliceの公開鍵を用いて$(K_A)^b = g^{ab} \mod p$を計算

AliceとBobしかわからない共通鍵$g^{ab} \mod p$を交換することができた.

DH Key Exchangeのエッセンス

漏れてもいいK_A, K_Bを元に, Alice, Bobしか計算できない$g^{ab} \mod p$を生成することができる.

- Alice, Bobしか計算できないことを保証するには?

Hardness Assumptionを元に安全性が担保されている.

(難しさを保証するためのgとpの条件)

1. pは1024ビット以上の素数で, p-1の約数の中にpに近いサイズの素数qがある.
    - p = 2q + 1 となるような素数qがあるようなpとか.
2. gは生成元($i = 1, \ldots, q-1$に対して$g^i \neq 1 \mod p$なる値)

DH Key Exchangeの安全性

以下のHardness Assumptionsのもとで安全

- Discrete Log Assumption(DLA)
- Diffie-Hellman Assumption(DHA)

Discrete Log Assumption (DL仮定)

離散対数問題(DLP)

> 生成元$g, p, g^a mod p$が与えられた時, aを求める問題

DLA

> DLPが難しいという仮定

DLAが崩れると, $K_A = g^a$からaを求められてしまうため, DH Key Exchangeが崩壊

DLPの例

巡回群$G = 1, 4 \mod 5, g = 4, p = 5, g^a mod p = 1$となるaを求める.
$4^1 \mod 5 = 4, 4^2 \mod 5 = 1$, よって$a = 2$

DLAの用途: g^aの一方向性

- g, aが与えられた時, g^aの計算は繰り返し2乗法(qiita, 繰り返し2乗法、行列累乗)で$O(log(a))$ で計算できる.
  - e.g. $3^{22} = 3^{16+4+2} = 3^{2^4} * 3^{2^2} * 3^{2^1} = (3^{2^1})^*(3^{2^1})^2 * ((3^{2^1})^2)^2$
- しかし, g, g^aからaを求めるには基本的にaを全探索するしかない. $O(a)$

Computational Diffie-Hellman Assumption(CDH仮定)

DH Problem(DHP)

> $g, p, g^a \mod p, g^b \mod p$ が与えられた時, $g^{ab} \mod p$を求めよ

CDH Asumption

> DHPは困難であるという仮定

Diffie-Hellman Key Exchangeで公開されている情報は以下の4つ

- $g, p, K_A = g^a \mod p, K_B = g^b \mod p$

これらを用いて攻撃者が秘密鍵$g^{ab} \mod p$を効率よく計算できたら暗号が機能しない.

DH Key ExchangeにおけるHarness Assumptionの関係

- 問題の難しさはDLP $\geq$ DHP
  DLPが解けたら, DHPも解ける.
  $\because g, g^a \mod p$からaを求められれば(DLP), K_Bから$g^{ab} \mod p$を求めることができる.
- 仮定の強さはDLA $\leq$ DHA
  攻撃者をDHPすら解けないだろうと甘く見ている

DH Key Exchangeの注意

Man in the Middle 攻撃に対して脆弱

- AliceとBobの間にEveがいるとき, EveはAliceとBobに対してそれぞれ別の公開鍵を送ることができ, 盗聴可能となる.

その他の重要なAssumptions

RSA Assumption(RSA仮定)

RSA問題

> n = pq (p, qは相異なる素数), 整数e, dをde = 1 (mod (p-1)(q-1))を満たすように選ぶ.
> この時, $c = Enc(m) = m^e \mod n$が与えられた時, mを求める問題

RSA Assumption

> RSA問題は困難

- n = pqの因数分解ができればRSA問題は簡単に解ける.
- 因数分解以外の方法でRSA問題を簡単に解ける可能性もある.

Learning with Errors (LWE)

格子暗号で用いられるHardness Assumption

> LWE: 有限体F_p上で考える.
> n*m次行列A, n次元ベクトルs, m次の誤差ベクトルeに対して,
> A, B = As+eが与えられた時, sを求める問題

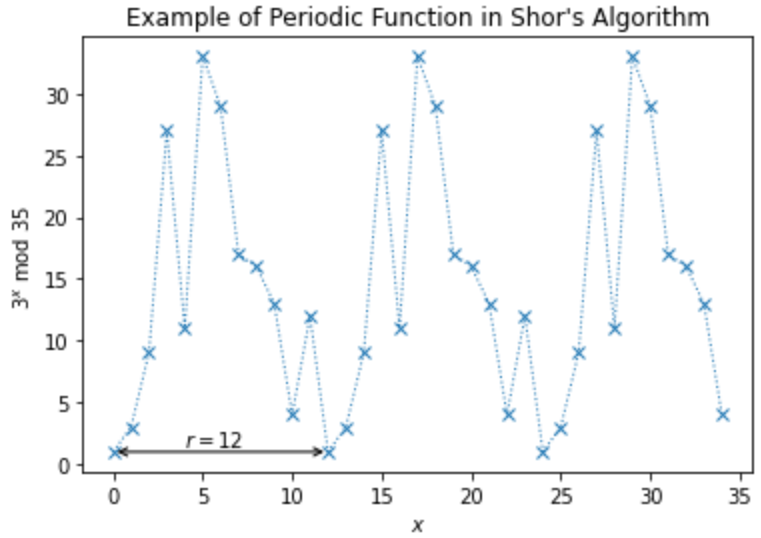
- e=0ならただの連立方程式を解く問題$O(n^3)$だが, eがランダムな値を取るため, この問題は困難であるという仮定.
- 単純に解くならeの全探索が必要.

Ref.

acompany, 完全準同型暗号1(格子暗号とは?)

余談: 耐量子暗号としての格子暗号(1/3)

- 量子計算機を用いて素因数分解を効率的に解くショアのアルゴリズムが発明(1994).
  - 整数Nの素因数分解が$O((\log N)^2 * \log\log N)$のゲート数で求められる.
- ショアのアルゴリズムは, 素因数分解を位数発見問題($a^r = 1 \mod N$ のrを解く問題)に帰着して効率的に解く.
  - 素因数分解だけでなく, 離散対数問題も適用可能



出典: ibm, shors-algorithm

余談: 耐量子暗号としての格子暗号(2/3)

ショアのアルゴリズムによるHardness Assumptionの崩壊

- 量子計算機は古典計算機と計算モデルが異なるため今までのHardness Assumptionが通用しないケースがある. 量子コンピュータ実機を用いた離散対数問題の求解実験に成功, NICT
  現在
- 現在広く普及しているRSA暗号や楕円曲線暗号が危機

Post Quantum Cryptography(PQC)の台頭

量子計算機で解きにくい問題(LWEなど)を元にした格子暗号が耐量子暗号の候補として注目されている.

余談: 耐量子暗号としての格子暗号(3/3)

ショアのアルゴリズムの限界

- 当面の間は大きな問題に対してショアのアルゴリズムが動かせるほどの量子コンピュータはできないと言われている.
  - 2012年で21の素因数分解できるくらい. (nature, Experimental realisation of Shor's quantum factoring algorithm using qubit recycling)
- 理由: 誤り訂正のために大量(数千万以上)の物理量子ビットが必要, etc
  - 2023年現在は数百ビット(ibm newsroom)

余談: 公開鍵方式における注意点(Chosen Plaintext Attack)

Chosen Plaintext Attack(CPA)

> - 攻撃者は, 公開鍵Kを用いて平文mを暗号化した暗号文c=Enc(K,m)を得ることができる.
> - 攻撃者は, いろんな平文mを暗号化した暗号文c=Enc(K,m)のリストLを持っておく
> - 誰かが送信した暗号文cをLの要素と比較して解読できる.

CPAの回避のために, Encは確率的アルゴリズムでなければならない
→ ElGamal暗号はCDH仮定を元にした, Enc時に乱数rを用いる確率的アルゴリズムの公開鍵暗号方式

まとめ

- 数論・代数学の上に暗号技術が成り立っている
- 様々なHardness Assumptionsが用いられている
- Assumptionsにも多様性がある
- 安全な暗号を考えるためには考慮すべき点が大量にある

Reference

- 暗号理論入門 第3版, J.A.ブーフマン
- クラウドを支えるこれからの暗号技術, 光成 滋生
- 代数学1 群論入門, 雪江明彦
- Introduction to Cryptography, Vipul Goyal, https://www.cs.cmu.edu/~goyal/s18/15503/scribe_notes/