符号理論･暗号理論

- No.14 暗号安全性 -

渡辺 裕

Coding Theory / Cryptography

- No.14 Security of Cryptography -

Hiroshi Watanabe

暗号解読

- 暗号文単独攻撃 Ciphertext-only attack (COA)
  - 暗号文のみを用いて, 平文を求める攻撃
- 既知平文攻撃 Known-plaintext attack (KPA)
  - 既知の平文に対応する暗号文を得られる条件で, 暗号文から平文を求める攻撃
- 選択平文攻撃 Chosen-plaintext attack (CPA)
  - 任意の平文に対応する暗号文を得られる条件で, 暗号文から平文を求める攻撃
- 選択暗号文攻撃 Chosen-ciphertext attack (CCA)
  - 任意の暗号文(ただし解読対象の暗号文は除く)に対応する平文を得られる条件で, ある暗号文から平文を求める攻撃

Cryptanalysis

- Ciphertext-only attack (COA)
  - cryptanalyst has access only to a collection of ciphertexts or codetexts
- Known-plaintext attack (KPA)
  - attacker has a set of ciphertexts to which he knows the corresponding plaintext
- Chosen-plaintext attack (CPA)
  - attacker can obtain the ciphertexts corresponding to an arbitrary set of plaintexts of his own choosing
- Chosen-ciphertext attack (CCA)
  - attacker can obtain the plaintexts corresponding to an arbitrary set of ciphertexts of his own choosing

計算量的安全性 (1)

- 暗号解読に必要なアルゴリズムの計算量に着目した暗号の安全性に関する概念の一つ
  - ある暗号を解読するための計算量が多項式時間に収まらない場合, その暗号は計算量的に安全
  - 実際に製品に組み込まれている暗号では鍵長などのパラメータが固定されていて解読計算量は定数時間
  - しかし, パラメータ選択時に現状及び今後の計算機能力の見積りを行い, 安全性を保ちたい期間内には解読可能にならないような値を設定
- 安全性の十分条件を与える情報理論的安全性よりは弱い安全性
- 必要条件を与えるに過ぎない統計量的安全性よりは強い安全性

Computationally Secure (1)

- A concept on security based on required algorithmic computational time to solve cipher
  - Cipher is computationally secure when calculation time to solve cipher stays less than polynomial time
  - In reality, cipher embedded in commercial products use fixed parameters such as key lengths. Thus, calculation time to solve is constant time
  - Set parameters not to be solved less than a desired safe computational time by estimating current and future computational power
- Less secure than information-theoretic security, which gives sufficient condition for security
- More secure than stochastic computation security, which gives necessary condition for security

計算量的安全性 (2)

- 計算量的安全性の概念
  - 暗号の解読や署名の偽造などを計算問題として定式化
  - これを解く最も効率のよいアルゴリズムの計算量をもって暗号の安全性の評価尺度とする
  - 暗号解読に必要な計算量が利用できる計算機の能力に比較して膨大であり，現実的時間では実行不可能である場合に計算量的に安全
- マージン
  - 計算機の能力は時間と共に向上
  - 計算機の計算能力の増大はある程度予測可能
  - 計算機能力の増大に備えた十分なマージンを持たせ，所定期間内に暗号解読が現実化することのないような値を選択

Computationally Secure (2)

- Concept of Computationally Secure
  - Formulate solving cipher or falsifying of signature
  - as a computational problem
  - Set security measure of cipher by the amount of computational time of algorithm solving efficiently
  - It is said computationally secure when computational time to solve cipher is extremely large than available computational power in reality
- Margin
  - Computational power increases as times go by
  - Power increase can be predicted to some extent
  - Set enough margin for power increase, select values by which cipher cannot be solved in a certain period

情報理論的安定性

- 暗号が情報理論的な意味で無条件に安全であるためには「平文サイズ≦鍵サイズ」を満たすことが必要十分条件
  - シャノン「秘匿系での通信理論」(1949)
  - この条件を満たすワンタイムパッドは情報理論的に安全
  - どれだけの暗号文を集めても，無限大の計算能力を持ってしても，解読できない
  - 平文と同じサイズの秘密鍵を事前に通信者間で共有する必要があり非現実的

Information-theoretic Security

- Necessary and sufficient condition to be secure for cipher in an information-theoretic sense is “plain-text size ≦ key size”
  - “”Communication Theory of Secrecy Systems” C. Shannon (1949)
  - Onetime pad to satisfy the condition above is information-theoretic secure
  - It cannot be solvable by collecting any ciphers and even by infinite computational power
  - However, it needs to keep the same size private key with plain-text in both sender and receiver, so that it is not realistic.

証明可能安全性 (1)

- 証明可能安全性
  - ある計算問題の計算量の下界を与える一般な解法は未だなく，ある暗号方式がどのような解読方法についても安全であるということを証明するのは困難
  - 暗号方式が計算量的安全性を備えていることを主張するためには，暗号を解読する問題をよく知られた困難だと考えられている計算問題に帰着させる
  - 根拠となる計算問題への帰着を証明することで示される安全性を証明可能安全性という
    - Ex. NP困難，ナップサック問題

Provable Security (1)

- Provable security
  - There is no general solution to give lower bond of a computational problem, so that it is difficult to prove that a cipher is secure to any decipher methods.
  - To affirm that a cipher is computationally secure, resolve decipher problem to some difficult calculation problem
  - Safety shown by proving resolved calculation problem is called provable security
    - Ex. NP-hard problem, Knapsak problem

証明可能安全性 (2)

- 応用例
  - ナップサック問題を利用した暗号方式
    - Merkle-Hellmanナップサック暗号
  - NP困難ではないが多項式時間の解法は存在しないと考えられている問題が利用されている公開鍵暗号
    - 素因数分解問題(RSA暗号, Rabin暗号)
    - 離散対数問題(ElGamal暗号)
    - DH判定問題(Cramer-Shoup暗号)

Provable Security (2)

- Application
  - Cipher using Knapsack problem
    - Merkle-Hellman knapsack cipher
  - Public key cipher using problem that it is not NP-hard but polynomial time solution may not exist
    - Prime number factorization problem (RSA cryptography, Rabin cryptography)
    - Discrete logarithmic problem (ElGamal encryption)
    - DH decision problem (Cramer-Shoup encryption)

暗号の危殆化

- 計算量的安全性の低下要因
  - 新たな解読手法が発見され解読に必要な計算量が減少する場合
  - 新型の計算機の登場により, 解読に利用できる計算機能力が増大する場合
- 計算量的に安全なパラメータ (2000)
  - 解読に要する計算量が 2^{64} 以下の場合には安全とは言えず, 2^{100} 以上であれば当面の安全性を有する

Reservation of Cipher

- Caused by low computational security
  - New algorithm is found and it makes decipher computational time shorter
  - New computer is developed and computational power is increased
- Parameter example for computational security (2000)
  - It is not said secure if computational cost is less than 2^{64}, secure if it is more than 2^{100} so far