修士論文審査用資料

推測盗聴者を伴う暗号システムの符号化定理

数理情報学専攻 46217 林 裕
指導教員 山本 博資教授

2006 年 2 月 7 日

概要

従来、シャノン暗号システムの安全性は暗号文を知った盗聴者の秘密情報に対する条件付エントロピー，つまり秘密情報の曖昧さの大きさで評価されていた．これに対して Merhav と Arikan は，盗聴者が正しい秘密情報を見つけるまでの推測回数を安全性指標として提案している．また Merhav は暗号文を盗聴した盗聴者が最も最適な推測値を求め，それが正しい確率を安全性指標として提案している．

一方，Yamamoto は相関情報源の一方を受信者が復号し，もう一方を盗聴者に対して安全にしたいというモデルを条件付エントロピーを用いて評価している．

本論文では，Yamamoto の提案した相関情報源を扱う暗号システムを Merhav らが提案した推測回数や推測確率を用いた安全性指標で評価する．

1　はじめに

暗号方式の一つである共通鍵暗号方式をモデル化したものにシャノン暗号システムがある．このモデルの安全性指標として，暗号文を盗聴したときの秘密情報に対する条件付エントロピーがよく用いられる．しかし，上記の安全性指標以外に Merhav と Arikan[2] は盗聴者の推測回数を用いた安全性指標を提案している．これは盗聴者が暗号文から正しい平文を見つけるまでにいくつの平文を推測しなければならないかによって安全性を測る指標であり，推測回数が大きければ大きいほど盗聴に対して安全であるといえる．Merhav–Arikan はより一般的に推測回数の ρ 次のモーメントの期待値を考え，その指数部のレートを指標として用いている．また，推測回数がある一定の値を超える確率（大偏差挙動）も安全性指標として提案している．Merhav–Arikan はこの値が鍵レートと情報源のタイプによって定まることを示した．また，推測回数が最大になるとき，つまりこの安全性指標の下で最も安全となるときの鍵レートも求めている．一方，Merhav[1] は盗聴者が暗号文から平文を正しく推測する確率を用いた安全性指標を提案している．この安全性指標の下，推測確率をある値より小さくするために必要な鍵の長さを示し，実際にその鍵の長さを持つ暗号化方法を構成している．

一方，Yamamoto[4] は条件付エントロピーによる安全性指標を用いて，実際に秘密にしたい情報と相関のある情報を伝送する場合の符号化定理を証明している．この場合，秘密情報と伝送情報の間の相互情報量と同じ鍵レートで最も安全となることが示されている．

本稿では，Merhav-Arikan が提案した推測回数の ρ 次のモーメント，推測回数の大偏差挙動，Merhav が提案した推測確率の各々を安全性指標を用いて Yamamoto の提案した相関情報源を扱うシャノン暗号システムの安全性を評価する．

2　相関情報源と推測盗聴者を伴う暗号システムモデル

2.1　推測回数を用いた安全性指標

相関のある長さ N の情報源出力 $\boldsymbol{X}$ と $\boldsymbol{Y}$ を, 長さ K の鍵 $\boldsymbol{U}$ を用いて暗号化する．このときの暗号化関数を f とし，暗号文 $Z = f(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{U})$ を送信する．ここで確率変数 $\boldsymbol{X}, \boldsymbol{Y}, Z, \boldsymbol{U}$ は有限離散アルファベット $\mathcal{X}^N, \mathcal{Y}^N, \mathcal{Z}$ および $\mathcal{U}^K$ 上の値をとるものとする．この鍵 $\boldsymbol{U}$ と暗号化関数 f は送信者と受信者で共有しているものとする．暗号文を受け取った受信者は正しい鍵 $\boldsymbol{U}$ と復号化関数 f^{-1} を用いて情報を $\hat{\boldsymbol{Y}} = f^{-1}(Z, \boldsymbol{U})$ により復号する．また，鍵のレートを $R = K/N$ とする．

盗聴者は暗号化関数 f を知っているものとし，暗号文 Z から秘密情報 $\boldsymbol{X}$ を推測する．このときの推測戦略を $g = \{\hat{\boldsymbol{X}}_1(Z), \hat{\boldsymbol{X}}_2(Z), \cdots\}$ とする．この戦略 g において正しい秘密情報にたどりつくまでの推測回数を $G_g^N(\boldsymbol{X}|Z)$ とする．つまり，$\hat{\boldsymbol{X}}_i(Z) = \boldsymbol{X}$ となるときの i が推測回数となる．この推測回数の ρ 次モーメントを求め，次のような指標を定める．

$$C_2 \equiv \lim_{N\to\infty} \sup_f \inf_g \frac{1}{N} \log \mathrm{E}[G_g^N(\boldsymbol{X}|Z)^\rho] \qquad (1)$$

この安全性指標 C_2 が鍵レート R による関数になることが次の定理で示される．

定理 2.1 Y の確率分布を $P(y)$，Y が与えられたときの X の条件付確率分布を $W(x|y)$, X, Y の同時確率分布を $P{\cdot}W(x, y)$ とする．このとき，任意の $\rho > 0$ に対して，$C_2 = C_2^*(R, \rho)$ が成り立つ．ただし，

$$C_2^*(R, \rho) \equiv \max_{Q,V} [\rho h(Q, V, R) - D(Q \cdot V \| P \cdot W)] \qquad (2)$$

$$h(Q, V, R) \equiv \min\{H(QV), R + H(QV) - I(Q, V)\} \qquad (3)$$

であり，Q は Y の任意の確率分布，V は Y に対する X の任意の条件付確率分布，QV は Q と V で定まる X の分布，$Q \cdot V$ は X, Y の同時確率分布である．

この定理より，式 (2) において，

$$\max_{Q,V}[\rho H(QV) - D(Q\cdot V\|P\cdot W)] \tag{4}$$

を達成する確率分布 Q^*, V^* に対して $R \geq I(Q^*, V^*)$ であるときは推測回数は最大となり，条件付エントロピーによる安全性指標で最も安全となる場合と同様に相互情報量が関係する値となる．

なお，秘密情報 $\boldsymbol{X}$ と伝送情報 $\boldsymbol{Y}$ が全く同じであるときは，Merhav–Arikan が示した定理 [2, Theorem 1] と一致する．

次に推測回数がある値を超える確率（大偏差挙動）による安全性指標を次式で定義する．ここで，L はセキュリティレベルである．

$$F_2 \equiv \lim_{N\to\infty}\inf_f\sup_g\left[-\frac{1}{N}\log\Pr\{G_g^N(\boldsymbol{X}|Z)\geq 2^{NL}\}\right] \tag{5}$$

この安全性指標 F_2 について以下の定理が成り立つ．

定理 2.2 Y の確率分布を $P(y)$，Y が与えられたときの X の条件付確率分布を $W(x|y)$, X, Y の同時確率分布を $P{\cdot}W(x,y)$ とする．このとき，任意の $L > 0$ に対して，$F_2 = F_2^*(R, L)$ が成り立つ．

$$F_2^*(R,L) \equiv \min_{\substack{Q,V\\ h(Q,V,R)\geq L}} D(Q\cdot V\|P\cdot W) \tag{6}$$

ここで，Q は Y の任意の確率分布，V は Y に対する X の任意の条件付確率分布，また $Q\cdot V$ は (X,Y) の同時確率分布である．

最後に，推測回数の ρ 次モーメントの期待値 $C_2^*(R,\rho)$ と推測回数の大偏差挙動 $F_2^*(R,L)$ はフェンシェル–ルジャンドル変換 (Fenchel–Legendre transform) によってお互いに関係している事を示す．

定理 2.3 Y の確率分布を P とし，Y が与えられたときの X の条件付確率分布を W とする．このとき，任意の鍵レート R に対して，以下の関係が成り立つ．

$$C_2^*(R,\rho) = \sup_{L>0}\,[\rho L - F_2^*(R,L)] \tag{7}$$

$$F_2^*(R,L) = \sup_{\rho>0}\,[\rho L - C_2^*(R,\rho)] \tag{8}$$

2.2 推測確率を用いた安全性指標

本節では，暗号文 z を知った盗聴者が秘密情報 $\boldsymbol{x}$ を推測し，それが正しい確率を用いた安全性指標に関する定理を示す．盗聴者の推測値として最適なものは，z に対して最も現れやすい秘密情報 $\boldsymbol{x}$ という意味で，次式を満たす $\hat{\boldsymbol{x}}$ である．

$$\hat{\boldsymbol{x}} = \arg\max_{\boldsymbol{x}} P(\boldsymbol{x}|z) \tag{9}$$

よって，暗号文 z を知ったときに盗聴者の推測が成功する確率は，次式で表される．

$$P_c = \sum_z P(z)\max_{\boldsymbol{x}} P(\boldsymbol{x}|z) \tag{10}$$

この推測確率 P_c を $2^{-N\lambda}$ より小さくするための必要条件として，次の定理が成り立つ．また，符号化は $\boldsymbol{x}, \boldsymbol{y}$ の両方を見て行うので，使用する鍵の長さを $K(\boldsymbol{x},\boldsymbol{y})$ とする．

定理 2.4 与えられた正数 $\lambda > 0$ に対し，もし $P_c < 2^{-N\lambda}$ であるなら，任意の正数 $\epsilon > 0$，任意の $\boldsymbol{Y}$ のタイプ Q と $\boldsymbol{y}$ に対する $\boldsymbol{x}$ の任意の条件付タイプ V について以下の式が成り立つ．

$$\begin{aligned}&\big|\mathcal{T}_{Q\cdot V}\cap\{(\boldsymbol{x},\boldsymbol{y})\colon K(\boldsymbol{x},\boldsymbol{y})\\ &\leq N([\lambda - H(V|Q) + H(\bar{V}|QV) - D(Q\cdot V\|P\cdot W)]_+ - \epsilon)\}\big|\\ &\qquad\qquad \leq 2^{o(N)-N\epsilon}|\mathcal{T}_{Q\cdot V}|\end{aligned} \tag{11}$$

ただし，$[a]_+ \equiv \max\{0, a\}$ である．

また，実際に推測確率の指数オーダーを $2^{-N\lambda}$ に保ちつつ，鍵の長さは

$$K(\boldsymbol{x},\boldsymbol{y}) = N[\lambda - D(Q\cdot V\|P\cdot W) - H(V|Q) + H(\bar{V}|QV)]_+ \tag{12}$$

となるような暗号化方法も構成した．

3 まとめ・今後の課題

本稿では，情報量的安全性に基づいた共通鍵暗号方式のモデルであるシャノン暗号システムにおいて，送信者が相関のある情報源を持ち，そのうち一方を受信者に対して送り，もう一方を秘密にする場合を考え，盗聴者に対する暗号システムの安全性を盗聴者が正しい秘密情報を見つけるまでの推測回数，または盗聴者が正しく秘密情報を推測する確率を用いて評価した．

今後の課題としては，今まで盗聴者に対する条件付エントロピーを用いて評価されていた様々な暗号システムモデルにおいて推測盗聴者を伴う場合の符号化定理を示す必要がある．さらに，その安全性指標の下で最も安全な場合に必要な鍵レートを求め，条件付エントロピーによる安全性指標の下で完全秘匿を達成する鍵レートと比較することが考えられる．

参考文献

[1] N. Merhav,“A Large-Deviations Notion of Perfect Secrecy,” *IEEE Trans. Inform. Theory*, Vol. 49, pp. 506-508, No. 2, Feb. 2003.

[2] N. Merhav and E. Arikan,“The Shannon Cipher System with a Guessing Wiretapper,” *IEEE Trans. Inform. Theory*, Vol. 45, pp. 1860-1866, 1999.

[3] 植松 友彦: 現代シャノン理論－タイプによる情報理論. 培風館, 東京, 1998.

[4] H. Yamamoto,“Coding Theorems for Shannon’s Cipher System with Correlated Source Outputs, and Common Information,” *IEEE Trans. Inform. Theory*, Vol. 40, pp. 85-95, No. 1, Jan. 1994.