卒業論文要旨

AHP とファジイ演算を用いた暗号の選択支援法

（知能情報システム学）　濱田　優

１．緒言

現在世界で使用されている暗号の数は非常に多く、どの用途にどの暗号を使えば良いかは明確になっているとはいえない。暗号にはそれぞれ特徴がある。たとえば、回路規模、暗号強度、処理速度は暗号選択での要素ともなる特徴である。本研究ではそれら特徴に対して独自の基準項目を設け、電子政府用に推奨された共通鍵暗号等[1]を AHP(Analytic Hierarchy Process) [2],[3] とファジィ演算により評価する方法を検討した。

２．方法

２．１．AHP における基準項目

CRYPTREC REPORT 2000[1]を参考に種々の 64bit 暗号、128bit 暗号をそれぞれソフトウェア実装とハードウェア実装の場合について以下に述べる点を基準として比較し、AHP により数値化した。

１）ソフトウェア実装

・安全性：線形／差分攻撃耐性，代数的及びその他攻撃耐性，アバランシュ特性

・処理速度：データランダム化部の処理速度，データランダム化部及び鍵スケジュール部の処理速度

２）ハードウェア実装

・安全性：繰り返し段数（ラウンド数）と攻撃可能段数の比較による安全性，線形／差分攻撃耐性，代数的及びその他攻撃耐性，アバランシュ特性

・処理速度：データランダム化部及び鍵スケジュール部の処理速度

・回路規模

２．２．手順

①元データより、各基準項目に対する各対象暗号の一対比較行列を得る。

②上記の一対比較行列から、各対象暗号の各基準項目に対する幾何平均を得、さらにその総和が１となる様に正規化する。

③安全性、処理速度など基準項目の一対比較行列を作成し、手順②と同様の手段により正規化した基準項目幾何平均を得る。

④正規化後の基準項目の幾何平均と暗号に対する正規化後の幾何平均をそれぞれ乗じ、さらにそれらの総和を求め、これを AHP による評価とする。

⑤各暗号に対し、５つの三角形のメンバーシップ関数を重みとして基準項目に対して与え、暗号の AHP における評価の「あいまいさ」を検証する。

３．評価例

評価対象の暗号は以下に示す通りである。

[64bit] CIPHERUNICORN-E, FEAL-NX, Hierocrypt-L1, MISTY1※, Triple DES※

[128bit] Camellia※, CIPHERUNICORN-A, Hierocrypt-3, RC6, SC2000, MARS, Rijndael

※ ループアーキテクチャで速度優先または回路規模優先の２つを評価

基準項目に対して、安全性、処理速度、回路規模の順に重みをつけた例において 64bit 暗号のソフトウェア実装では MISTY1、ハードウェア実装では TDES(回路規模優先)が特に高い評価を得、128bit 暗号のソフトウェア実装では RC6、ハードウェア実装では Camellia がそれぞれ高い評価を得た。64bit ハードウェア実装(図１)における TDES(回路規模優先)は AHP による評価は高いが、メンバーシップ関数で三角形が他の三角形と大部分で重なり、新たな基準項目が増えるなどした時、評価が変わる可能性の高いことが予測された。逆に、128bit ソフトウェア実装(図２)における RC6 は AHP での評価も高い。かつ、メンバーシップ関数の三角形も他の三角形とあまり重なっていないので、評価に含まれるあいまいさは少ないといえる。

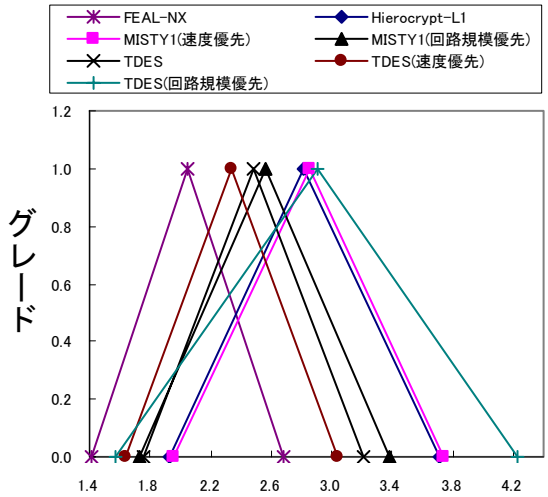

図１　64bit ハードウェア実装評価

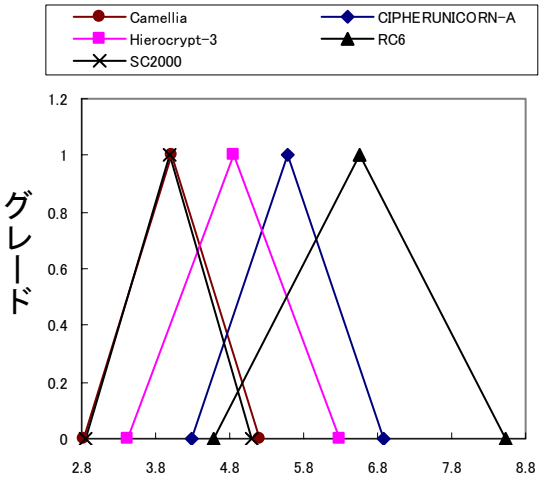

図２　128bit ソフトウェア実装評価

４．結言

AHP による評価は評価者の価値観に大きく依存している。本研究で提案した暗号選択支援法は、重みを暗号利用ユーザーが実状に応じてメンバーシップ関数として設定することによりユーザーにとって最適な暗号の選択を支援するものである。総合評価を表す三角形の幅が狭く、かつ AHP の評価が高いものがユーザーに適している暗号として推奨できる。

参考文献

[1] 情報処理振興事業協会セキュリティセンター編, IPA CRYPTREC REPORT2000, 2001.

[2] 八巻直一, 高井英造, 問題解決のための AHP 入門, 日本評論社, 2005.

[3] 高萩栄一郎, 中島信之, Excel で学ぶ AHP 入門 問題解決のための階層分析法, オーム社, 2006.