

解説



暗号安全性の最近の動向

7. 文献紹介†

藤岡 淳††

1. はじめに

ここでは、本特集で引用された論文やその他の重要な文献について、その内容を概説する。

まず、DES と FEAL に関しては、以下の文献を参照されたい。

- ・ Data Encryption Standard, Federal Information Processing Standards Publication 46, National Bureau of Standards, U.S. Department of Commerce (1977).
- ・ Miyaguchi, S., Kurihara, S., Ohta, K. and Morita, H.: Expansion of FEAL Cipher, *NTT Review*, Vol.2, No.6, pp.117-127 (1990).

また、暗号技術の紹介と最新動向に関する良書として、

- ・ Schneier, B.: *Applied Cryptography Second Edition*, John Wiley & Sons, Chichester (1996).

を推薦する。

2. インターネット・セキュリティ

インターネットにおいて中心的な役割を担う UNIX の安全性については、様々な解説書が存在している。

- ・ Garfinkel, S. and Spafford, G.: *Practical UNIX Security*, O'Reilly & Associates, Sebastopol (1991).

山口英監訳: UNIX セキュリティ, アスキー出版 (1992).

- ・ Curry, D. A.: *UNIX System Security*, Addison-Wesley, Massachusetts (1992).

小林憲司訳: UNIX システムセキュリティ, ソフトバンク (1993).

また、最近、電子メールのセキュリティに関する

解説書も出版された。

- ・ Schneier, B.: *E-Mail Security*, John Wiley & Sons, Chichester (1995).

力武健次監訳, 道下宣博訳: E-Mail セキュリティ, オーム社 (1995).

最後に、インターネットセキュリティについての優れた解説として、

- ・ 山本和彦: 転ばぬ先のセキュリティ, *UNIX Magazine* (連載中), アスキー.

をあげておく。これは、雑誌連載のため、読みやすく、最新の内容が掲載されている。

3. 社会での暗号技術の取り扱いと Clipper Chip について

Clipper Chip に用いられている暗号方式の強度に関しては、

- ・ Brickell, E., Denning, D. E., Kent, S. T., Maher, D. and Tuchmann, W.: SKIPJACK Review: Interim Report, posted to the *Sci. Crypt* newsgroup on August 1, 1993.

に報告されている。

一方、Clipper Chip を用いながら、捜査当局による(正当な)盗聴を無効にするような不正手段が発見されており、それに関する文献として、たとえば、

- ・ Blaze, M.: Protocol Failure in the Escrowed Encryption Standard, *Proceedings of The 2nd ACM Conference on Computer and Communications Security*, pp.59-67 (1994).

があげられる。

4. 暗号の解読・攻撃法

4.1 差分攻撃法

差分攻撃法は、Biham と Shamir によって提案され、最初 DES (8 段) と FEAL-8 に対するデモが行われ、論文としては、

† Bibliography by Atsushi FUJIOKA (NTT Information and Communication Systems Laboratories).

†† NTT 情報通信研究所

- ・ Biham, E. and Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems, *Proceedings of CRYPTO '90* (1990).

が発表された。その後、さらに研究が進み、ついに、16 段の DES の理論的解読に成功したのである。

- ・ Biham, E. and Shamir, A.: Differential Cryptanalysis of the full 16-round DES, *Proceedings of CRYPTO '92* (1992).

また、解説書として、

- ・ Biham, E. and Shamir, A.: *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, New York (1993).

がある。

4.2 線形攻撃法

一方、線形攻撃法は日本の暗号研究者の松井らにより提案された。まず、当初は FEAL に対する攻撃法として示された。

- ・ Matsui, M. and Yamagishi, A.: A New Method for Known Plaintext Attack of FEAL Cipher, *Proceedings of EUROCRYPT '92* (1992).

さらに、この手法が DES に対しては、差分攻撃法よりも効率的であることが示された。

- ・ Matsui, M.: Linear Cryptanalysis Method for DES Cipher, *Proceedings of EUROCRYPT '93* (1993).

また、線形攻撃法による DES に対する計算機実験の結果は、

- ・ Matsui, M.: The First Experimental Cryptanalysis of the Full 16-round DES, *Proceedings of CRYPTO '94* (1994).

に示されている。

4.3 関連する話題

ここでは、差分攻撃法・線形攻撃法に関連する話題をいくつか紹介する。

最近、差分攻撃法・線形攻撃法を組み合わせた差分線形攻撃が提案されている。

- ・ Langford, S. K. and Hellman, M. E.: Differential-Linear Cryptanalysis, *Proceedings of CRYPTO '94* (1994).

また、差分攻撃法と線形攻撃法が離散フーリエ変換を介して密接に関連するという理論的に興味深い結果が示されている。

- ・ Chabaud, F. and Vaudenay, S.: Links Between

Differential and Linear Cryptanalysis, *Proceedings of EUROCRYPT '94* (1994).

これら差分攻撃法、線形攻撃法の発見を契機として、この2つの攻撃法に対して安全性が理論的に保証されている暗号系を設計しようとの動きが出てきており、

- ・ Nyberg, K. and Knudsen, L. R.: Provable Security Against a Differential Attack, *Journal of Cryptology*, Vol. 8, No. 1, pp.27-37 (1995).

- ・ 松井, 時田, 反町, 山岸, 市川: 差分解読法と線形解読法に対する証明可能安全性をもつ実用ブロック暗号, *Proceedings of the 1996 Symposium on Cryptography and Information Security*, 4C (1996).

が、代表的な論文としてあげられる。

最後に、安全な暗号系の設計を目的とした国際学会が定期的に開催されるようになった。最新情報は予稿集

- ・ Anderson, R. (Ed.): *Fast Software Encryption*, Lecture Notes in Computer Science, No.809, Springer-Verlag, Berlin (1994).

- ・ Preneel, B. (Ed.): *Fast Software Encryption*, Lecture Notes in Computer Science, No.1008, Springer-Verlag, Berlin (1995).

- ・ Gollmann, D. (Ed.): *Fast Software Encryption*, Lecture Notes in Computer Science, No.1039, Springer-Verlag, Berlin (1996).

を参照することをお薦めする。

5. おわりに

暗号安全性に関する代表的な文献を紹介した。

読者の方々が、この特集から暗号理論の面白さと現状に対する知識を深めていただけたら幸いです。
(平成8年2月13日受付)



藤岡 淳 (正会員)

昭和37年生。昭和60年東京工業大学電気・電子工学科卒業。平成2年同大学院理工学研究科電気・電子工学専攻博士後期課程修了。工学博士。同年日本電信電話(株)入社。平成5年から6年までスイス連邦工科大学客員研究員。現在、NTT 情報通信研究所主任研究員。情報セキュリティ、ネットワーク・セキュリティなどの研究開発に従事。平成4年度電子情報通信学会業績賞、小林記念特別賞受賞。電子情報通信学会会員。