数理解析研究所講究録
1120巻 1999年 58-58

実用的暗号系のための厳密な安全性評価尺度

Exact treatment of security for practical cryptosystems

櫻井 幸一
Kouichi SAKURAI

九州大学 システム情報科学研究科 情報工学専攻
〒812-8581 福岡県 福岡市 東区 箱崎 6-10-1
http://tcslab.csce.kyushu-u.ac.jp/~sakurai/

キーワード: 公開鍵暗号, 電子署名, 厳密安全性, 漸近的安全性

概要

実際に暗号がインターネット上で、利用されている今日、暗号解読の脅威が高まってきている。したがって、理論的に安全性が保証された暗号方式の設計が、暗号理論における重要な研究課題となっている。

暗号系（特に公開鍵暗号）の理論的安全性は、その暗号系を破るアルゴリズムから、基本となる問題（素因数分解や離散対数問題）を計算するアルゴリズムへの還元（reduction）効率に関する漸近論で議論されてきた。しかし、実際に暗号系が、特定のパラメータサイズで利用される今日、これまでの”多項式時間”や”十分大きなサイズの入力”といった漸近論では、現実的な安全性を議論するには、不十分であることが指摘されている。

このため、アルゴリズム間の還元効率を細分し、具象的安全性(Concrete secueity)の導入や、その最適化である厳密安全性(Exact security)が議論されはじめた。本論では、これら最近の安全性評価尺度の概要を説明すると同時に、暗号だけでなく、一般のアルゴリズム論への拡張とその有効性を探る。

参考文献

[Be97b] M. Bellare. “Practice-oriented provable-security,” Proceedings of First International Workshop on Information Security (ISW 97), LNCS Vol. 1396, E. Okamoto, G. Davida and M. Mambo eds., Springer Verlag, 1998.

[BeRo93b] M. Bellare and P. Rogaway. “Random oracles are practical: A paradigm for designing efficient protocols” Extended abstract in Proc. First Annual Conference on Computer and Communications Security, ACM, 1993.

[BeRo94] M. Bellare and P. Rogaway. “Optimal asymmetric encryption – How to encrypt with RSA” in Advances in Cryptology - Eurocrypt 94 Proceedings, LNCS Vol. 950, A. De Santis ed, Springer-Verlag, 1995.

[BeRo96a] M. Bellare and P. Rogaway. “The exact security of digital signatures: How to sign with RSA and Rabin,” in Advances in Cryptology - Eurocrypt 96 Proceedings, LNCS Vol. 1070, U. Maurer ed, Springer-Verlag, 1996.

[MiRe99] S.Micali and L.Reyzin “Improving the eaxct security of digital signature schemes,” Avaivable from Theory Crypto library of MIT.

[OhOk98] K.Ohta and T.Okamoto, “On concrete security of treatment of signatures derived from identification,” in Advances in Cryptology - Crypto 98 Proceedings, LNCS Vol. 1462, H.Krawczyk ed, Springer-Verlag, 1996.