モーバイル環境に適した圧縮／暗号通信方式（２）
－圧縮／暗号同時実行アルゴリズム－

3W－6

吉浦裕*　宝木和夫*　橋本尚**

（株）日立製作所システム開発研究所*　（株）日立製作所ソフトウェア事業本部**

１．まえがき

インターネット、モーバイル環境では、帯域が狭く盗聴が容易なWANや無線通信を用いるため、圧縮と暗号の両者を必要とする場合が多い。ところが、従来、圧縮と暗号は独立にシステム化され、両者の統合システムが提供されていないので、様々な実用上の問題が生じている。特に、モデム通信の場合、圧縮機能がモデムにあるため、暗号化が圧縮の前に実行される。そのため、暗号化によりデータの規則性が失われ、圧縮の効果が発揮されなかった。以上から、圧縮と暗号の統合システムが必要である。

一方、圧縮にはデータをランダム化する等の暗号的要素がある。そこで、単に圧縮と暗号を組合せるのではなく、両者の融合により、新たな利点を生み出せる可能性がある。本論文では、圧縮・暗号統合システムの中核技術として、両者の融合方法を論ずる。

従来の圧縮と暗号の融合の研究では、平文符号と圧縮符号の対応関係を暗号化することにより、圧縮データを間接的に暗号化していた[1-3]。ところが、これらの方法については、平文符号の頻度統計に基づく解読、選択平文攻撃の可能性が指摘されている[2]。本論文では、圧縮の性質の利用により暗号の強度、効率を向上する方法を提案する。

２．圧縮および暗号の性質

２．１　圧縮の性質

ここでは、広く実用化されている動的な可逆圧縮を検討対象とする。圧縮の性質として、以下が挙げられる。

（１）エラー伝搬が不可避である。例えば、圧縮データの１ビットが反転すると、それ以降の部分について、正確な復元は困難である。

（２）データがランダム化される。例えば、平文における文字の頻度等の情報は保存されない。

（３）平文符号と圧縮符号の対応関係は複数通り可能である[3]。

２．２　暗号の性質

ここでは、圧縮の対象となる大量データの暗号化に適した秘密鍵暗号を検討対象とする。暗号方式の設計では、各種の解読方法に対する防御が重要な要件となる。従来最も多く用いられている解読方法は鍵の全数探索であるが、最近では、より効率的な差分解読[4]および線形解読[5]が注目されている。差分、線形解読は、一つの鍵による平文と暗号文の対を複数収集し、統計処理により鍵を推定するものである。差分、線形解読に対する従来の防御方法としては、暗号段数の増加が主である。ところが、暗号段数の増加には、処理時間の増加という問題があった。

３．圧縮と暗号の融合

３．１　融合の方針

（１）ブロック間依存伝搬による解読への防御

従来の暗号方式では、エラー伝搬を回避するために、平文を６４ビット程度のブロック毎に独立して処理していた。ところが、前記のように、圧縮ではエラー伝搬が不可避なので、圧縮との組合せの場合、暗号でエラー伝搬を回避する意味がない。そこで、ブロック間の処理の依存伝搬を許容することにより、暗号方式設計の制約を緩和し、差分、線形解読を防止する。

（２）圧縮のランダム性を利用した暗号段数の削減

圧縮には、平文をランダム化する性質がある。また、圧縮の途中で平文符号と圧縮符号の対応関係を切り替えることにより、ランダム性をさらに増大することができる。この性質を利用して、所定のランダム性を達成するための暗号段数を削減し、処理効率を向上する。

３．２　融合方法（図１）

（１）ブロック間依存伝搬による鍵スケジュール

差分、線形解読では、一つの鍵による平文と暗号文の対を複数収集し、統計処理を行う。そこで、これを防ぐには、ブロック毎に鍵をランダムに変更すればよい。こ

Compression/Encryption Communication Method for Mobile Environments (2)

Hiroshi Yoshiura*, Kazuo Takaragi*, Hisashi Hashimoto**
Systems Development Laboratory, Hitachi Ltd.*
Software Development Center, Hitachi Ltd.**

方法として、前ブロックの暗号化の中間結果に依存して、次ブロックの暗号化の鍵を生成する方法を提案する。

（2）乱数による初期鍵の変更

上記の方法だけでは最初のブロックの鍵（初期鍵）が固定となる。そのため、最初のブロックの平文と暗号文を、複数のデータにわたって収集することにより、差分、線形解読が可能である。そこで、データ毎に乱数を発生し、その値に依存して初期鍵を生成する。乱数発生には、暗号のOFBモードを用いる。以上の（1）、（2）により、差分、線形解読を防止できる。

（3）平文符号と圧縮符号の対応関係の切換

ブロック毎の鍵に依存して、平文符号と圧縮符号の対応関係を切り替える。その結果、圧縮のランダム性を増すことができ、所定の暗号強度を達成するための暗号段数を削減できる。

4．MULTI2暗号[6]を例とする評価

（1）MULTI2暗号の概要

MULTI2暗号の8段以上の場合については、差分解読以外の解読法は見つかっていない。ところが、差分解読を用いると、8段の場合、40000の平文、暗号文の対から鍵を推定できる[7]。（実用版のMULTI2暗号では32ないし128段が使用されている。実用版については、一切の解読法は見つかっていない）。

（2）暗号強度向上の評価

まず、初期鍵に対する差分、線形解読を考える。乱数を128ビットとすると、その周期は約2^{64}である。そこで、MULTI2 8段の解読に必要な40000の平文、暗号文の対を収集するためには、$2^{64}\times40000$個のデータを暗号化する必要があるが、これは事実上不可能である。2番目以降のブロックの鍵は、入力データに依存して変化するので、その推定は初期鍵の場合以上に困難である。以上から、提案方式によりMULTI2 8段の解読を防止できる。

（3）処理性能向上の評価

上記により、段数を従来の32から8に削減できる。また、圧縮のランダム性を利用して、さらに段数を減らせる。一方、提案方式により新たに加わる処理は、乱数発生および、平文符号と圧縮符号の対応関係の切換である。前者は、1データに1回しか実行しないので、その処理量は無視できる。また、後者の処理量も無視できるほど小さい[3]。以上から、提案方式により、暗号の処理量を従来の1／4以下に削減できる（圧縮の処理量は従来と同じである）。

5．むすび

本論文では、圧縮の性質を利用して暗号の強度、効率を向上する方式を提案した。MULTI2暗号を例として、提案方式の有効性を評価し、実用上十分な暗号強度が従来の1／4以下の暗号処理量で達成できることを示した。

【参考文献】

[1] 樽川ほか：算術符号を用いた秘密鍵暗号方式，信学技法 IT91-34 (1991).

[2] 松岡，森井，中野：暗号と圧縮の組合わせに関する一考察，SCIS94-8C (1994).

[3] 横田，田中：データ圧縮機能を備えたストリーム暗号の提案，ISEC95-43 (1995).

[4] E. Biham, A. Shamir：Differential Criptanalysis of DES-like Cryptosystem, CRYPTO 90 (1990).

[5] 松井：DES 暗号の線型解読法(1)～(3)，SCIS93-3C (1993).

[6] 宝木，佐々木，中川：情処学会マルチメディア通信と分散処理研究会，40-5 (1989).

[7]松井，山岸：秘密鍵暗号方式の確率的解読法に関する考察，信学論A, Vol. J77-A, No.3 (1994).

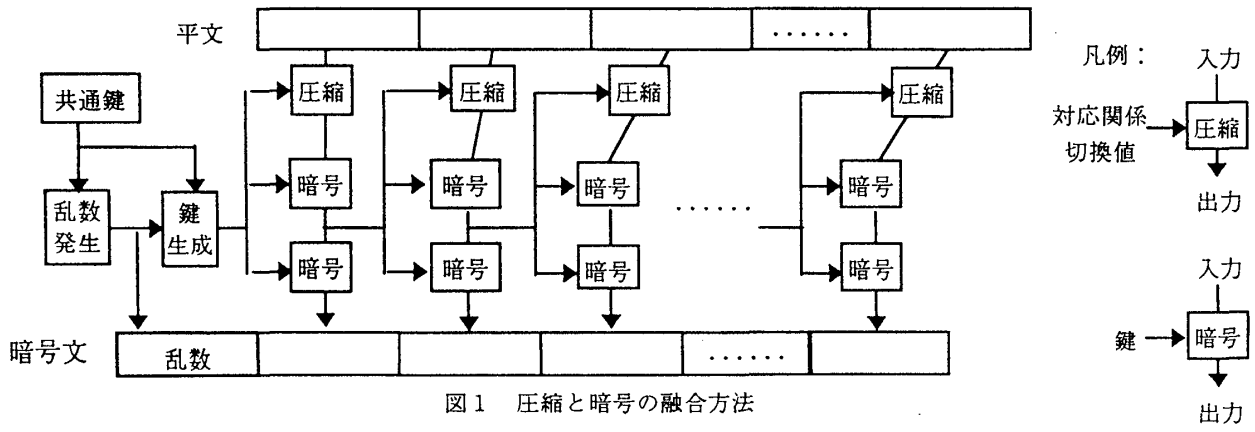

図1　圧縮と暗号の融合方法