AVR1317 : XMEGA 組み込みDES加速器の使い方

要点

■ DES反復を実行するXMEGA® CPUへの命令ｾｯﾄ拡張
・ﾃﾞｰﾀ暗号化規格(DES)に従った64ﾋﾞｯﾄ ﾃﾞｰﾀの暗号化と解読の能力

1. 序説

XMEGA系統はDES反復を実行する拡張命令ｾｯﾄを持っています。本応用記述は素早い準備と行動のための例と共にXMEGAのDES命令機能の基本的な機能を記述します。その上、Cとｱｾﾝﾌﾞﾘ言語で書かれたﾄﾞﾗｲﾊﾞ ｲﾝﾀｰﾌｪｰｽが含まれています。

2. 理屈

暗号は秘密情報を保つ芸術または科学であり、暗号の手段を隠すか、または暗号鍵を保全することに基づいています。使用した手段の安全性に基くだけの方法は主に歴史的興味で、現実世界の要求に合致しません。現代の方法は暗号化と解読の制御に鍵を使用します。一致する鍵なしに、掻き回されたﾒｯｾｰｼﾞやﾃﾞｰﾀを平文に整列することはできません。

暗号鍵に基く方法は対称と非対称の2つに分けられます。対称法は暗号化と解読に対して同じ鍵を用い、一方非対称法は異なる鍵を使用します。最も学ばれ、多分最も広範囲に広まっている対称法はDESです。

2.1. ﾃﾞｰﾀ暗号化規格(DES)

ﾃﾞｰﾀ暗号化規格(DES)は元来1970年代に開発され、後に米国標準技術局(US NIST:US National Institute of Standards and Technology)によって標準規格に転化されました。DESは8ﾋﾞｯﾄのﾊﾟﾘﾃｨを含む64ﾋﾞｯﾄ鍵を使用する対称暗号法です。64ﾋﾞｯﾄのﾃﾞｰﾀ塊で操作する塊暗号です。入力の塊の各々は図2-1.で図解されるように処理されます。DES法はもはや安全に対して考慮されておらず、従ってその使用は推奨されません。DES自身は本資料の後ろで示されるもっと安全な仕組みで改造されて再使用することができます。

DES法はﾊﾟﾘﾃｨﾋﾞｯﾄのために56ﾋﾞｯﾄの効率的な鍵長を持ちます。これは可能な鍵の組み合わせ数が以下であることを意味します。

$2^{56} = 72,057,594,037,927,936 = 7.206 \times 10^{16}$

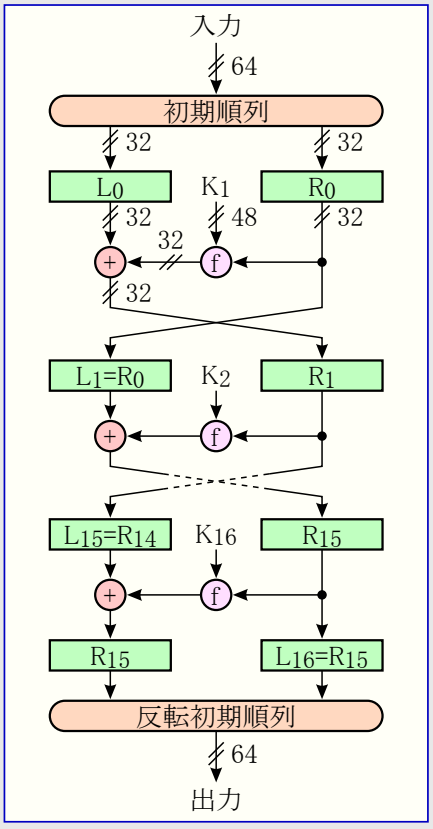
脆弱な鍵の(存在の)ために安全性は更に減少します。

図2-1.は単一ﾃﾞｰﾀ塊がどう符号化されるかを図解します。最初に入力ﾋﾞｯﾄの順番が順列関数に従って変更されます。その後に下位32ﾋﾞｯﾄ(R0)は上位32ﾋﾞｯﾄ(L0)と分離されて処理されます。これらは暗号鍵の異なる補助組(Kn)を使用する各段の16処理段階です(図2-1.では1,2,16段階だけが図解されます)。最後に初期順列関数に対して逆に変更されます。

解読法は暗号化法と同じで、鍵の補助組(Kn)の順が逆にされるだけです。

DES法自体の完全な記述は本応用記述の範囲外です。この方法の完全な仕様についてはFIPS標準規格を参照してください。

図2-1. DES法に従った暗号化の流れ



http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

8ﾋﾞｯﾄ AVR® マイクロ コントローラ

応用記述

本書は一般の方々の便宜のため有志により作成されたもので、ATMEL社とは無関係であることを御承知ください。しおりのはじめにでの内容にご注意ください。

Rev. 8105A-04/08, 8105AJ4-03/14

2.2. 3重ﾃﾞｰﾀ暗号化規格(3DES)

3重ﾃﾞｰﾀ暗号化規格(3DES)は3回のDES使用に基き、従って鍵長は56から168ﾋﾞｯﾄに増加します。3DESはDESよりも非常に強力ですが、3倍遅くなります。より新しい新暗号化規格(AES)は著しく高い安全余裕を提供し、可能ならばその使用が推奨されます。

3DES法は3つの56ﾋﾞｯﾄ暗号鍵を使用します。従って組み合わせ数は以下のように増加します。

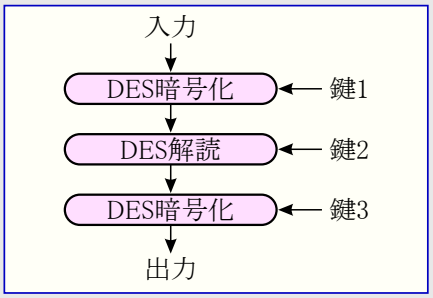
$2^{168} = 3.741 \times 10^{50}$

しかし、DES法での弱点のために効果的な安全性提供は112ﾋﾞｯﾄだけです。

3DESはANSI® x9.52で定義されています。暗号化の流れは右で図解されます。

暗号化中、入力は初めに最初の鍵で暗号化され、その後に第2の鍵で解読され、最後に第3の鍵で暗号化されます。解読中、鍵の順と符号化/解読塊の順が逆にされます。

図2-2. 3DES法に従った暗号化の流れ



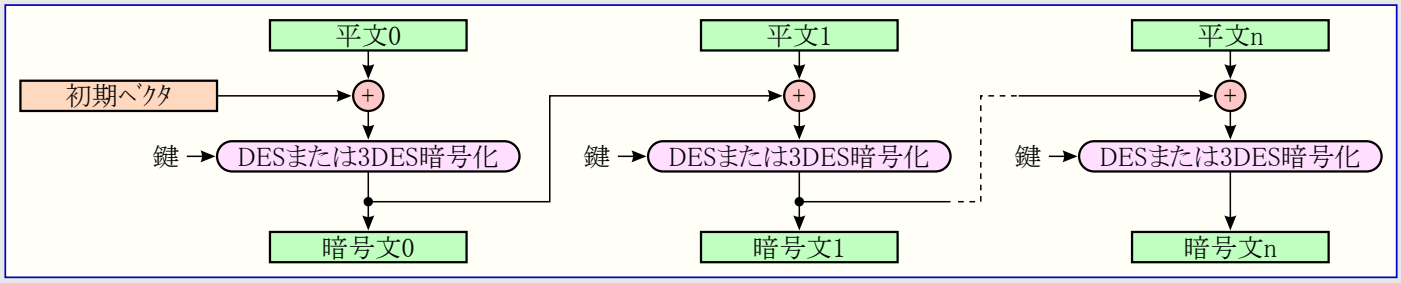
2.3. 暗号塊連鎖(CBC:Cipher Block Chaining)

DESと3DESは塊暗号で、この方法は固定量のﾃﾞｰﾀ塊で操作することを意味します。既知の入力塊と一定の暗号鍵に関して、その出力は常に同じです。この情報は暗号ｼｽﾃﾑの攻撃を欲する誰かにとって有用な提供かもしれません。

同じ平文の塊を違う暗号文の塊に暗号化させるのに一般的に使用される方法があります。そのような方法は暗号塊連鎖(CBC)と呼ばれます。

CBCは先行塊が全ての後行塊に影響を及ぼすような暗号塊を接続する方法です。これは(XOR操作の)結果を暗号化する前で、最初に平文の塊と直前の暗号文の塊でXOR操作を実行することによって成し遂げられます。これは1つの暗号文ﾋﾞｯﾄが依存するところの平文ﾋﾞｯﾄ数を増します。

図2-3. CBC暗号化



3. DES加速器

DES加速器はXMEGA CPUへの命令ｾｯﾄ拡張で、DES反復を実行します。64ﾋﾞｯﾄのﾃﾞｰﾀ塊(平文または暗号文)はCPUのR0～R7ﾚｼﾞｽﾀに置かれ、一方(ﾊﾟﾘﾃｨ ﾋﾞｯﾄを含む)完全な64ﾋﾞｯﾄ鍵はR8～R15ﾚｼﾞｽﾀに置かれます。1つのDES命令実行はDES法に於ける1周を実行します。正しい暗号文または平文を増やす(への変換を進める)ために16周実行されなければなりません。中間結果は各DES命令後にR0～R15ﾚｼﾞｽﾀ ﾌｧｲﾙ内に格納されます。命令のｵﾍﾟﾗﾝﾄﾞ(K)はどの周回が実行されるのかを決め、ﾊｰﾌｷｬﾘｰ(H)ﾌﾗｸﾞが暗号化または解読のどちらを実行するのかを決めます。

初期順列と反転初期順列が毎回反復実行されるため、中間結果はFIPS標準規格と異なります。これは暗号文または平文の最終結果に影響を及ぼしません。補助的情報についてはXMEGA手引書をご覧ください。

4. ﾄﾞﾗｲﾊﾞ実装

本応用記述はCｲﾝﾀｰﾌｪｰｽを持つｱｾﾝﾌﾞﾘ言語で実装されたDES基本ﾄﾞﾗｲﾊﾞの一括ｿｰｽ ｺｰﾄﾞを含みます。それはIAR Embedded Workbench® ｺﾝﾊﾟｲﾗで書かれています。

DESﾄﾞﾗｲﾊﾞはDES,3DESとCBCの暗号化と解読を支援します。

DESﾄﾞﾗｲﾊﾞが高性能ｺｰﾄﾞでの使用に対して意図されていないことに注意してください。それはDES加速器使用の開始に際するﾗｲﾌﾞﾗﾘとして設計されています。より多くの詳細についてはﾄﾞﾗｲﾊﾞのｿｰｽ ｺｰﾄﾞとﾃﾞﾊﾞｲｽのﾃﾞｰﾀｼｰﾄを参照してください。

4.1. ﾌｧｲﾙ

一括ｿｰｽ ｺｰﾄﾞは4つのﾌｧｲﾙから成ります。

- DES_driver_speed.s90 ：速度最適化DES加速器ﾄﾞﾗｲﾊﾞ ｿｰｽ ﾌｧｲﾙ
- DES_driver_size.s90 ：量最適化DES加速器ﾄﾞﾗｲﾊﾞ ｿｰｽ ﾌｧｲﾙ
- DES_driver.h ：DES加速器ﾄﾞﾗｲﾊﾞ ﾍｯﾀﾞ ﾌｧｲﾙ
- DES_example.c ：DES加速器ﾄﾞﾗｲﾊﾞを使用するｺｰﾄﾞ例

利用可能なﾄﾞﾗｲﾊﾞ ｲﾝﾀｰﾌｪｰｽ関数とそれらの使用の完全な概要についてはｿｰｽ ｺｰﾄﾞの資料を参照してください。課題に対して希望する最適化任意選択のﾄﾞﾗｲﾊﾞをｲﾝｸﾙｰﾄﾞしてください。

4.2. Doxygen資料化

全てのｿｰｽ ﾌｧｲﾙはDoxygenを使用する自動資料生成用に準備されています。Doxygenは特別なｷｰﾜｰﾄﾞを使用してｿｰｽ ｺｰﾄﾞを分析することによって、ｿｰｽ ｺｰﾄﾞから資料を作成するﾂｰﾙです。Doxygenについてのより多くの詳細に関してはhttp://www.doxygen.orgを訪ねてください。予めｺﾝﾊﾟｲﾙされたDoxygen資料は本応用記述に伴うｿｰｽ ｺｰﾄﾞと共に供給され、ｿｰｽ ｺｰﾄﾞ ﾌｫﾙﾀﾞのreadme.htmlﾌｧｲﾙから利用可能です。

本社

Atmel Corporation
2325 Orchard Parkway
San Jose, CA 95131
USA
TEL 1(408) 441-0311
FAX 1(408) 487-2600

国外営業拠点

Atmel Asia
Unit 1-5 & 16, 19/F
BEA Tower, Millennium City 5
418 Kwun Tong Road
Kwun Tong, Kowloon
Hong Kong
TEL (852) 2245-6100
FAX (852) 2722-1369

Atmel Europe
Le Krebs
8, Rue Jean-Pierre Timbaud
BP 309
78054 Saint-Quentin-en-
Yvelines Cedex
France
TEL (33) 1-30-60-70-00
FAX (33) 1-30-60-71-11

Atmel Japan
104-0033 東京都中央区
新川1-24-8
東熱新川ﾋﾞﾙ 9F
ｱﾄﾒﾙ ｼﾞｬﾊﾟﾝ株式会社
TEL (81) 03-3523-3551
FAX (81) 03-3523-7581

製品窓口

ｳｪﾌﾞｻｲﾄ
www.atmel.com

技術支援
avr@atmel.com

販売窓口
www.atmel.com/contacts

文献請求
www.atmel.com/literature

本応用記述はATMELのAVR1317応用記述(doc8105.pdf Rev.8105A-04/08)の翻訳日本語版です。日本語では不自然となる重複する形容表現は省略されている場合があります。日本語では難解となる表現は大幅に意訳されている部分もあります。必要に応じて一部加筆されています。頁割の変更により、原本より頁数が少なくなっています。

必要と思われる部分には( )内に英語表記や略称などを残す形で表記しています。

青字の部分はﾘﾝｸとなっています。一般的に赤字の0,1は論理0,1を表します。その他の赤字は重要な部分を表します。