シ研打合わせ資料

楕円スカラ倍のICF3 μによる性能評価

1. 目的

ICF3 LSiでの演算は、IPで直接演算する場合とは異なり、IP-ICF3間のデータ転送オーバーヘッドがあるため、なるべく1個のμファンクションでより多くの演算を行えるようなμファンクション セットを用意することが性能上、得策である。

一方、μのインプリメントの工数が増大するなどのデメリットがあるため、mod Pの四則演算のμファンクションセットを用意し、アセンブラ命令により暗号演算を実現することも考えられる。ここでは、性能と工数のトレードオフを検討するために、4つのμファンクションセットについて、楕円スカラ倍の性能評価を行う。

2. 性能評価前提

・1cycは、とくにことわらない限りμのcycを示し、下記のような関係になっている。

1 cyc = 2 ICF cyc = 8 IP cyc

・bit長　：160 , 256 , 320bit

・スカラ値：bit長の X'AAA…A'

・同期命令 1μファンクションのオーバーヘッドは100cyc と仮定する。

根拠　EMD,DMD,TCBCE,TCBCD,GMAC命令の性能測定TMP実測値から最小二乗法により0BYTE長の場合のIP cyc数を求めた結果 758cyc～933cycであったため、ざっと800 IP cycとし、これをICF μcycに換算した結果 100cyc。

・ICF3 LSiにデータを保存してμファンクションを終了し、次のμファンクションでその結果を用いることはせず毎回データをIPに転送する。

・どのμファンクションも一律、3レジスタ IP→ICFに転送、1レジスタ ICF→IPに転送するものとする。

IP→ICF I/Fレジスタの転送レートは、8Byte/cyc

ICF I/Fレジスタ→IPの転送レートは、4Byte/cyc

ICF I/Fレジスタ→剰余演算器レジスタの転送レート 5.33Byte/cyc (8Byte/3ICFcyc)

剰余演算器レジスタ→ICF I/Fレジスタの転送レート 5.33Byte/cyc (8Byte/3ICFcyc)

IP←→ICF I/Fレジスタ間は、1レジスタ当たり、鍵長のデータ転送(8Byte単位)

ICF I/Fレジスタ←→剰余演算器レジスタ、1レジスタ当たり、128Byteのデータ転送

1レジスタのIP→ICF転送cyc数

160bit：24/8 + 128/5.33 = 27cyc
256bit：32/8 + 128/5.33 = 28cyc
320bit：40/8 + 128/5.33 = 29cyc

1レジスタのICF→IP転送cyc数

160bit：24/4 + 128/5.33 = 30cyc
256bit：32/4 + 128/5.33 = 32cyc
320bit：40/4 + 128/5.33 = 34cyc

1μファンクション発行によるデータ転送オーバーヘッド

160bit：27×3 + 30 = 111cyc
256bit：28×3 + 32 = 116cyc
320bit：29×3 + 34 = 121cyc

・モンゴメリ変換を用いる

・単体の有限体の加算、減算

bit長をkとする。

μコード　データ転送のオーバーヘッドが含まれる。

ミリコード 64bitの加算が1 IP cycで行えるものとすると 有限体加算 2×(k/64) IP cyc、有限体減算 3×(k/64) IP cyc

Mアセンブラ 32bitの加算が1 IP cycで行えるものとすると 有限体加算 2×(k/32) IP cyc、有限体減算 3×(k/32) IP cyc

	μコード		ミリコード		Mアセンブラ	
	加算	減算	加算	減算	加算	減算
160bit	214cyc	215cyc	0.75cyc	1.13cyc	1.25cyc	1.88cyc
256bit	219cyc	220cyc	1.00cyc	1.50cyc	2.00cyc	3.00cyc
320bit	224cyc	225cyc	1.25cyc	1.88cyc	2.50cyc	3.75cyc

上記の表より、明らかに加算・減算はIPで実行した方が高速であるためICFμでは行わない。

・スカラ倍のアルゴリズムにもよるが、ここではスカラ値の前提からk/2-1回の楕円加法、k-1回の楕円2倍の計算を行うものとする。

3. μファンクション セット

セット1	有限体 乗算、モンゴメリ乗算、有限体除算、Mアセンブラによる有限体 加減算
セット2	有限体 乗算、モンゴメリ乗算、有限体除算、ミリコードによる有減体 加減算
セット3	セット1 + 楕円加法、楕円2倍
セット4	セット3 + 楕円スカラ倍

4. 性能評価

各ｱﾙｺﾞﾘｽﾞﾑにおける楕円加法、楕円2倍、前後処理の有限体 加減乗除 演算数(回)
演算数の算出方法は、"並列化ﾌﾟﾛｼﾞｪｸﾃｨﾌﾞ"については付録C 参照、"通常"については、
定数倍を加法を用いて計算することを除けば公式の表記どおり。

開22G 12.5.29 谷口

AES状態 TWO FISH * RIJNDHEL ベルギー SERPENT

	ｱﾙｺﾞﾘｽﾞﾑ	加算	減算	乗算	ﾓﾝｺﾞﾒﾘ乗算	除算
楕円加法	通常	0	6	0	2	1
	並列化ﾌﾟﾛｼﾞｪｸﾃｨﾌﾞ	3	7	0	14	0
楕円2倍	通常	5	3	0	4	1
	並列化ﾌﾟﾛｼﾞｪｸﾃｨﾌﾞ	10	3	0	8	0
前後処理	通常	0	0	0	4	0
	並列化ﾌﾟﾛｼﾞｪｸﾃｨﾌﾞ	0	0	0	6	2

μﾌｧﾝｸｼｮﾝｾｯﾄと鍵長による加減乗除のcyc数
ｾｯﾄ1,2では、連続して演算する場合には不要な、ﾚｼﾞｽﾀｱｸｾｽがあるため +1cycを見積もった。

	加算			減算			ﾓﾝｺﾞﾒﾘ乗算			除算			1μﾌｧﾝｸｼｮﾝのｵｰﾊﾞｰﾍｯﾄﾞ合計		
鍵長	160bit	256bit	320bit	160bit	256bit	320bit	160bit	256bit	320bit	160bit	256bit	320bit	160bit	256bit	320bit
ｾｯﾄ1	1.25	2.00	2.50	1.88	3.00	3.75	85	133	165	8366	13331	16609	211	216	221
ｾｯﾄ2	0.75	1.00	1.25	1.13	1.50	1.88									
ｾｯﾄ3	3			4			84	132	164	8365	13330	16608			
ｾｯﾄ4															

	ｱﾙｺﾞﾘｽﾞﾑ	μﾌｧﾝｸｼｮﾝｾｯﾄ	回数 加算	減算	ﾓﾝｺﾞﾒﾘ乗算	除算	ﾌｧﾝｸｼｮﾝ数	性能 cyc数	ｾｯﾄ4に対する比
160bit	並列化ﾌﾟﾛｼﾞｪｸﾃｨﾌﾞ 楕円加法 79回 楕円2倍 159回	ｾｯﾄ1	1827	1030	2384	2	2386	727038	3.21
		ｾｯﾄ3					246	278493	1.23
		ｾｯﾄ4					1	226798	1
256bit	通常 楕円加法 127回 楕円2倍 255回	ｾｯﾄ1	1267	1526	1260	384	1648	5599076	10.23
		ｾｯﾄ3					386	5327633	9.74
		ｾｯﾄ4					1	5244473	9.59
	並列化ﾌﾟﾛｼﾞｪｸﾃｨﾌﾞ 楕円加法 127回 楕円2倍 255回	ｾｯﾄ1	2931	1654	3824	2	3834	1374222	2.51
		ｾｯﾄ2						1368810	2.50
		ｾｯﾄ3					390	631077	1.15
		ｾｯﾄ4					1	547053	1
320bit	並列化ﾌﾟﾛｼﾞｪｸﾃｨﾌﾞ 楕円加法 159回 楕円2倍 319回	ｾｯﾄ1	3667	2070	4784	2	4794	1898982	2.29
		ｾｯﾄ3					486	939619	1.13
		ｾｯﾄ4					1	830738	1

5. まとめ

性能的な観点からｾｯﾄ3か、ｾｯﾄ4を考えたい。
ｾｯﾄ4では非同期命令とし、ｽｶﾗ倍演算命令発行後、IPは別の処理を行うことでｼｽﾃﾑのﾊﾟﾌｫｰﾏﾝｽを向上させることが考えられる。
ｾｯﾄ3では1ﾌｧﾝｸｼｮﾝ当たりの処理量が小さすぎるため非同期命令とすることのｵｰﾊﾞｰﾍｯﾄﾞによる性能劣化が問題になると考える。
ただし、いまのところｾｯﾄ4で、IEEE 1363 で示されるのｽｶﾗ倍ｱﾙｺﾞﾘｽﾞﾑをｲﾝﾌﾟﾘﾒﾝﾄすることは難しいと考えられるため(除算ｱﾙｺﾞﾘｽﾞﾑを変更し、性能をさげればｲﾝﾌﾟﾘﾒﾝﾄできる可能性有り)ｾｯﾄ3にするかｾｯﾄ4にするかは、いまのところ決定できない。

6. 今後の課題

・楕円ｽｶﾗ倍をIP計算した場合の性能との比較、可能なら(ｿﾌﾄ)から入手

鍵ﾊﾟﾗﾒｰﾀ: 「Introduction of ECAES」 July 29,30 1999 Hisanori Mishima Hitachi Ltd. のAppendix 4. 5つ目

pは256bit

p = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFC2F
a = 0000000000000000000000000000000000000000000000000000000000000000
b = 0000000000000000000000000000000000000000000000000000000000000007
G = 04 79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798
483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8
n = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141

において

k = AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

の場合の、楕円ｽｶﾗ倍の k(x, y) 性能

上記のﾊﾟﾗﾒｰﾀでのｾｯﾄ4の試作μｺｰﾄﾞ(前後処理がない)のμｼﾐｭﾚｰｼｮﾝ実行結果は、481221cyc(付録B参照)
これに前後処理、ﾓﾝｺﾞﾒﾘ乗算6回、除算2回のcyc数、1μﾌｧﾝｸｼｮﾝのｵｰﾊﾞｰﾍｯﾄﾞ 216cycを追加すると508889cyc
(見積もり値は、547053cyc)
~~ただしこのﾊﾟﾗﾒｰﾀの場合、楕円加法の1/2倍が単純なｼﾌﾄ1bitｼﾌﾄで済むため数ﾊﾟｰｾﾝﾄ高速化可能~~