(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2010 年 7 月 22 日(22.07.2010)

PCT

(10) 国際公開番号
WO 2010/082629 A1

(51) 国際特許分類:
H03M 7/04 (2006.01) *G06F 7/49* (2006.01)

(21) 国際出願番号: PCT/JP2010/050420

(22) 国際出願日: 2010 年 1 月 15 日(15.01.2010)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2009-006797 2009 年 1 月 15 日(15.01.2009) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社　東芝 **(KABUSHIKI KAISHA TOSHIBA)** [JP/JP]; 〒1058001 東京都港区芝浦一丁目１番１号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 清水　秀夫 **(SHIMIZU, Hideo)** [JP/JP].

(74) 代理人: 鈴江　武彦，外 **(SUZUYE, Takehiko** et al.); 〒1050001 東京都港区虎ノ門１丁目１２番９号 鈴榮特許綜合事務所内 Tokyo (JP).

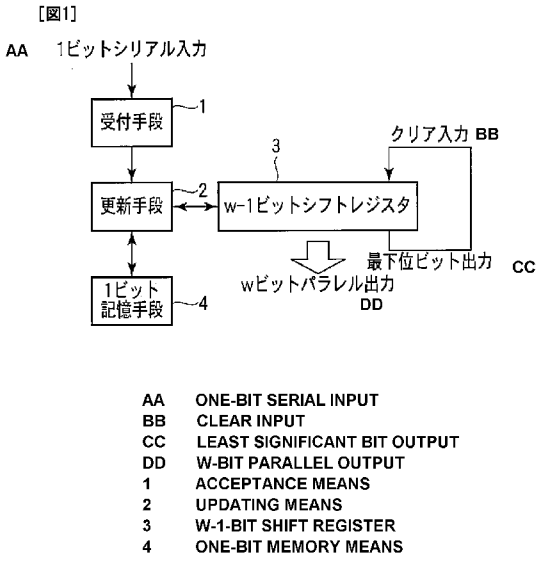
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告（条約第 21 条(3)）

(54) **Title**: NAF CONVERSION DEVICE

(54) 発明の名称 : ＮＡＦ変換装置



(57) **Abstract**: Provided is a scalable w-NAF conversion device with a small circuit size. The NAF device converts the binary expression of an integer into a redundant binary express expressed as a w-NAF. The device is equipped with an acceptance means which accepts the aforementioned binary expression of the integer one bit at a time starting with the least significant bit thereof; a memory means which stores a state value expressed with one bit; a shift register which stores a state value expressed with w-1 bits; and an updating means which references the one-bit value accepted by the aforementioned acceptance means, the state value in the aforementioned memory means, and the state value in the aforementioned w-1-bit shift register, determines the state of the aforementioned memory means and the state of the aforementioned w-1-bit shift register at the following time, and determines the w-bit parallel output at the present time.

(57) 要約:　回路規模が小さくスケーラブルなｗ－ＮＡＦ変換装置を提供する。整数の２進表現をｗ－ＮＡＦ表現された冗長２進表現に変換するＮＡＦ変換装置であって、前記整数の２進表現を下位から１ビットずつ受け付ける受付手段と、１ビットで表現される状態の値を記憶する記憶手段と、ｗ－１ビットで表現される状態の値を記憶するシフトレジスタと、前記受付手段が受け付けた１ビットの値と、前記記憶手段の状態の値と、前記ｗ－１ビットのシフトレジスタの状態の値を参照し、次の時刻における前記記憶手段の状態と前記ｗ－１ビットのシフトレジスタの状態とを決定し、現時刻におけるｗビットのパラレル出力を決定する更新手段と、を具備する。

WO 2010/082629 A1

明　細　書

発明の名称 ： ＮＡＦ変換装置

技術分野

[0001] 本発明は整数の２進表現を冗長２進表現に変換するＮＡＦ変換装置に関する。

背景技術

[0002] 乗数を冗長２進表現に変換してから乗算することで乗算を効率化できることについては、例えばＢｏｏｔｈの方法として１９５０年代には既に知られている（例えば非特許文献１、非特許文献２を参照）。最近では、暗号処理の高速化という文脈で冗長２進表現の１種であるＮＡＦが使われることが多い（例えば非特許文献３、非特許文献２を参照）。

[0003] ＮＡＦについては、例えば非特許文献２の第９８頁に説明されている。ＮＡＦとは、冗長２進表現の１種であり、整数ｋは唯一の対応するＮＡＦ表現ＮＡＦ（ｋ）をもつ。ＮＡＦ（ｋ）の非零の桁の数は任意の冗長２進表現の中でも最小であることが証明されている。非零の桁の数の平均は１／３である。

[0004] 通常の２進表現では、各桁に０または１の２種類の数字が現れるが、ＮＡＦでは－１，０，１の数字が現れるという違いがある。

[0005] ＮＡＦ表現では、引き続く２つの桁の少なくとも一方は０であるという特徴があり、密度が低い理由にもなっている。また、Ｎｏｎ－ａｄｊａｃｅｎｔ　ｆｏｒｍという名前の由来でもある。

[0006] 例として、２進数１１０１１（１０進では５９＝３２＋１６＋８＋２＋１）をＮＡＦに変換すると１０００－１０－１（６４－４－１＝５９）になる。

[0007] ４ビット以下の２進数をＮＡＦに変換した例を表１に示す。

[表1]

0	0
1	1
10	10
11	10−1
100	100
101	101
110	10−10
111	100−1
1000	1000
1001	1001
1010	1010
1011	10−10−1
1100	10−100
1101	10−101
1110	100−10
1111	1000−1

[0008] 整数ｋをＮＡＦ表現ＮＡＦ（ｋ）に変換するアルゴリズムはいくつも知られている。例えば、非特許文献４の第３９頁（表３．２）、非特許文献３の第９８頁（アルゴリズム３．３０）、非特許文献２の第１５１（アルゴリズム９．１４）に記載されている。

[0009] ＮＡＦの拡張としてｗ－ＮＡＦがある（例えば非特許文献３の第９９頁参照）。

[0010] ｗ－ＮＡＦと通常のＮＡＦの違いは、ｗ－ＮＡＦでは各桁に使える数字がもっと多くなっていることである。３－ＮＡＦであれば－３，－１，０，１，３の５種類を使用できる。上記のＮＡＦは２－ＮＡＦと考えることができる。

[0011] 以下、表２および表３にｗ－ＮＡＦの特徴を示す。

[0012] 表２は、各ＮＡＦで使う数字を一覧にしたものである。

[表2]

	使う数字	
2－NAF	－1，0，1	3種類
3－NAF	－3，－1，0，1，3	5種類
4－NAF	－7，－5，－3，－1，0，1，3，5，7	9種類
・・・		
w－NAF	-2^(w-1)-1,-2^(w-1)-3,...,-1,0,1,...,2^(w-1)-3,2^(w-1)-1	2^(w-1)+1種類

[0013] 但し、「^」はべき（冪）であり、例えば2^wは２のｗ乗を意味する。

[0014] 表３は、各ＮＡＦの非零の桁の密度を一覧にしたものである。

[表3]

	密度
2－NAF	1／3
3－NAF	1／4
4－NAF	1／5
・・・	
w－NAF	1／(w＋1)

[0015] ｗ－ＮＡＦでは、引き続くｗ個の桁の内、非零である桁は多くても１つであるという特徴がある。密度が低い方が処理する桁が少なくなるのでクロック数は少なくなるが、事前準備が多くなるのでトレードオフがある。

[0016] ｗ－ＮＡＦの変換アルゴリズムについては、非特許文献３の第１００頁（アルゴリズム３．３５）、非特許文献２の第１５３頁（アルゴリズム９．２０）がある。

[0017] 従来のＮＡＦ変換アルゴリズムについて検討する。

[0018] 非特許文献３のアルゴリズム３．３５や、非特許文献２のアルゴリズム９．２０は、任意のｗに対して適用できるというスケーラビリティの高さが特長であるが、反面、以下のような問題点がある。

[0019] ・逐次的にｋを入力することができない。つまり最初にｋを読み込んでおかなければならない。これはｋそのものを変更するからである。

[0020] ・ｋに対する変更は多倍長演算なので、回路規模が大きくなったり、１桁を求めるのに必要なクロック数が多くなる。

[0021] 非特許文献４の表３．２について、非特許文献４にはＮＡＦ変換であると

いう記述はないが、結果として出力されるものはＮＡＦ変換になっている。このアルゴリズムは上の２つのアルゴリズムのもつ欠点を持たない。つまり、逐次的にｋを処理できるし、多倍長演算も不要である。ただし、ｗ＝２の場合にしか適用できないのでスケーラビリティがないという問題がある。非特許文献２のアルゴリズム９．１４も同じ特長と欠点をもつ。

先行技術文献

非特許文献

[0022] 非特許文献1：A.D.Booth, "A signed binary multiplication technique", Quart. J. Mech. Appl. Math., 4, 2, 236-240, 1951.

非特許文献2："Handbook of Elliptic and Hyperelliptic Curve Cryptography", CRC, 2006

非特許文献3："Guide to Elliptic Curve Cryptography", Springer, 2003

非特許文献4：「算術演算のＶＬＳＩアルゴリズム」コロナ社，２００５

発明の概要

発明が解決しようとする課題

[0023] 上述したように、既に知られているＮＡＦ変換アルゴリズムには、スケーラビリティと回路規模が両立しないという問題点がある。

[0024] 本発明はかかる事情を考慮してなされたものであり、回路規模が小さくスケーラブルなｗ－ＮＡＦ変換装置を提供することを目的とする。

課題を解決するための手段

[0025] 本発明の一観点に係るＮＡＦ変換装置は、整数の２進表現をｗ－ＮＡＦ表現された冗長２進表現に変換するＮＡＦ変換装置であって、前記整数の２進表現を下位から１ビットずつ受け付ける受付手段と、１ビットで表現される状態の値を記憶する記憶手段と、ｗ－１ビットで表現される状態の値を記憶するシフトレジスタと、前記受付手段が受け付けた１ビットの値と、前記記憶手段の状態の値と、前記ｗ－１ビットのシフトレジスタの状態の値を参照し、次の時刻における前記記憶手段の状態と前記ｗ－１ビットのシフトレジ

スタの状態とを決定し、現時刻におけるｗビットのパラレル出力を決定する更新手段と、を具備することを特徴とする。

発明の効果

[0026] 本発明によれば、回路規模が小さくスケーラブルなｗ－ＮＡＦ変換装置を提供できる。特に、任意のｗについて異なる部分がほとんどない（シフトレジスタの長さだけ）ので、動的にｗを変更するといったことも可能である。また、回路規模は知られている２－ＮＡＦ専用の変換アルゴリズムよりも小型であり、さらには公知のｗ－ＮＡＦ変換アルゴリズムと較べても小型である。

図面の簡単な説明

[0027] [図1]ｗ－ＮＡＦ変換装置の機能構成を示すブロック図

[図2]２－ＮＡＦ変換装置を示す図

[図3]セレクタの記述方法の説明図

[図4]２－ＮＡＦ変換装置の変換例を示す図

[図5]３－ＮＡＦ変換装置を示す図

[図6]３－ＮＡＦ変換装置の変換例を示す図

[図7]４－ＮＡＦ変換装置を示す図

[図8]２～４－ＮＡＦ変換装置を示す図

[図9]２－ＮＡＦ状態遷移表を示す図

[図10]２－ＮＡＦ状態遷移図を示す図

[図11]３－ＮＡＦ状態遷移表を示す図

[図12]３－ＮＡＦ状態遷移図を示す図

[図13]４－ＮＡＦ状態遷移表を示す図

[図14]５－ＮＡＦ状態遷移表を示す図

発明を実施するための形態

[0028] 以下、図面を参照しながら本発明の実施形態を説明する。

[0029] 図１は、本発明の実施形態に係るＮＡＦ変換装置の機能構成を示すブロック図である。本装置は、１ビットシリアル入力を受け付ける受付手段１と、

受付手段１に接続される更新手段２と、更新手段２に接続され、ｗ－ＮＡＦ表現されたｗビットの値をパラレル出力するｗ－１ビットシフトレジスタ３と、更新手段２に接続される１ビット記憶手段４とを有する。なお、ＮＡＦ変換装置がハードウェアで構成される場合は、受付手段１は独立して設けられる必要はなく、信号線と更新手段とが接続される接続部分が該当することになる。

[0030] １ビット記憶手段４とｗ－１ビットシフトレジスタ３の初期値は０とする。

[0031] 本実施形態に係るＮＡＦ変換装置においては、ｗ－ＮＡＦ表現に変換すべき整数の２進表現を下位ビットから順にクロックに合わせて１ビットずつ受付手段１が受け付ける。この受け付けた値を１ビットシリアル入力という。１ビット記憶手段４とｗ－１ビットシフトレジスタ３の内容はクロック毎に、つまり１ビット入力される毎に更新手段２によって新たな内容に置き換えられる。

[0032] 更新手段２は更新前の１ビット記憶手段４とｗ－１ビットシフトレジスタ３の内容および１ビットシリアル入力に応じて、１ビット記憶手段４とｗ－１ビットシフトレジスタ３の新たな内容を計算する。また更新手段２はｗビットのパラレル出力を決定する。つまり、クロック毎にｗビットの変換結果が出力される。この際、有効な出力はｗ－１クロック後から出力される。なお、最下位ビット出力の値“１”は、ｗ－１ビットシフトレジスタ３をクリアするトリガーのクリア入力として、ｗ－１ビットシフトレジスタ３に与えられる。最下位ビット出力の値“１”がｗ－１ビットシフトレジスタ２に与えられると、ｗ－１ビットシフトレジスタ２の値はクリアされる。

[0033] 図２を参照して、図１のＮＡＦ変換装置をさらに具体化した２－ＮＡＦ変換装置を説明する。図２に示すように２－ＮＡＦ変換装置が有するＣは図１の構成における１ビット記憶手段４に対応する。同様に、Ｓ０は１ビットのシフトレジスタ３（ｗ＝２なのでｗ－１＝１ビット）に対応する。Ｙ１とＹ０は２ビットのパラレル出力に対応する。＋は１ビットの加算器であり、図

１の更新手段２の要素に対応する。

[0034] 特別な記号を図３で説明する。セレクタを図３のように記述することにする。つまり選択信号Ｓが１のとき出力はＣ＝Ａであり、Ｓが０のとき出力はＣ＝Ｂとなる。

[0035] 図１において、最下位ビット出力がｗ－１ビットシフトレジスタのクリア入力として与えられる構成は、図２において、パラレル出力の一部であるＹ０がセレクタの選択信号Ｓ０として与えられる構成に対応する。

[0036] ＣとＳ０の初期値は０である。Ｓ０が１のとき、Ｃの次の値は入力＋Ｃの下位ビットであり、Ｓ０の次の値は０であり、Ｙ１は入力＋Ｃの下位ビットであり、Ｙ０はＳ０つまり１となる。一方、Ｓ０が０のとき、Ｃの次の値は入力＋Ｃの上位ビットであり、Ｓ０の次の値は入力＋Ｃの下位ビットであり、Ｙ１は入力＋Ｃの下位ビットであり、Ｙ０はＳ０つまり０となる。なお、次のクロックのタイミングでＹ１の値がＳ０に書き込まれる。

[0037] 図４を参照して、この２－ＮＡＦ変換装置の実際の変換例を示す。図４はタイミングチャートの形式になっており、クロックが入るたびに色々な値が更新されている。図４においてｃｌｋはクロック、ｓｔａｒｔは開始信号、ｉｎは入力、ｃは１ビット記憶手段４、ｓは１ビットシフトレジスタ３、ｏｕｔは２ビットパラレル出力である。

[0038] ２進数１１１０１１（１０進では５９＝３２＋１６＋８＋２＋１）を入力した例を示す。ｉｎの行を見ると１１１０１１がクロック毎に下位から順に入力されていることが分かる。出力は入力より１クロック遅れている。

[0039] 出力ｏｕｔの読み方は、「００」または「１０」のとき「０」であり、「０１」のとき「１」であり、「１１」のとき「－１」である。

[0040] 上記のように０を表現する複数の出力があるが、全て偶数であり、最下位ビットが０のときは出力を０とみなすだけでよい。また、出力が０以外のときは、２ビットの２の補数表現になっていることに注意する。一般にｗ－ＮＡＦの場合は、出力の最下位ビットが０なら０、１ならｗビットの２の補数表現となる。出力の最下位ビット以外を最下位ビットとＡＮＤをとることで

きれいな０を出力することもできる。結果も下位から出力される。図４によれば、下位から順に－１０－１０００１と出力されていることが分かる。これは、上位から読むと１０００－１０－１であり、６４－４－１＝５９なので、元の２進数と同じ数を表現していることが分かる。元の２進数で非零の（１の）ビットは５個であるが、ＮＡＦ変換後は３個と非零の桁の数が減っている。ＮＡＦ変換では、出力のビット数は、最大で元のビット数＋１になることがあり、この例もそのようになっている。

[0041] 図５は図１のＮＡＦ変換装置をさらに別の例として具体化した３－ＮＡＦの変換装置を示している。図５に示すように３－ＮＡＦ変換装置が有するＣは図１の構成における１ビット記憶手段４に対応する。同様に、Ｓ１とＳ０は２ビットのシフトレジスタ３（ｗ＝３なのでｗ－１＝２ビット）に対応する。Ｙ２とＹ１とＹ０は３ビットのパラレル出力に対応する。＋は１ビットの加算器であり、図１の更新手段２の要素に対応する。図１において、最下位ビット出力がｗ－１ビットシフトレジスタのクリア入力として与えられる構成は、図５において、パラレル出力の一部であるＹ０が２つのセレクタのそれぞれの選択信号Ｓ０として与えられる構成に対応する。

[0042] 図２の２－ＮＡＦ変換装置と図５の３－ＮＡＦの変換装置とを較べると、Ｙ２とＳ１が増えただけである。動作は２－ＮＡＦ変換装置と同様である。

[0043] ＣとＳ０の初期値は０である。Ｓ０が１のとき、Ｃの次の値は入力＋Ｃの下位ビットであり、Ｓ１とＳ０の次の値は０であり、Ｙ２は入力＋Ｃの下位ビットであり、Ｙ１はＳ１であり、Ｙ０はＳ０つまり１となる。一方、Ｓ１が０のとき、Ｃの次の値は入力＋Ｃの上位ビットであり、Ｓ１の次の値は入力＋Ｃの下位ビットであり、Ｓ０の次の値はＳ１であり、Ｙ２は入力＋Ｃの下位ビットであり、Ｙ１はＳ１であり、Ｙ０はＳ０つまり０となる。

[0044] 図６を参照して、この３－ＮＡＦ変換装置の実際の変換例を示す。図６はタイミングチャートの形式になっており、クロックが入るたびに色々な値が更新されている。図６において、ｃｌｋはクロック、ｓｔａｒｔは開始信号、ｉｎは入力、ｃは１ビット記憶手段４、ｓは２ビットシフトレジスタ３、

ｏｕｔは３ビットパラレル出力である。

[0045] ２進数１１１０１１（１０進では５９＝３２＋１６＋８＋２＋１）を入力した例を示す。ｉｎの行を見ると１１１０１１がクロック毎に下位から順に入力されていることが分かる。出力は入力より２クロック遅れている。出力ｏｕｔの読み方は、「０００」，「０１０」，「１００」，「１１０」のとき、「０」であり、「００１」のとき「１」であり、「０１１」のとき「３」であり、「１０１」のとき「－３」であり、「１１１」のとき「－１」である。

[0046] 上記のように０を表現する複数の出力があるが、全て偶数であり、最下位ビットが０のときは出力を０とみなすだけでよい。また、出力が０以外のときは、３ビットの２の補数表現になっていることに注意する。結果も下位から出力される。下位から順に３００－１００１と出力されていることが分かる。これは、上位から読むと１００－１００３であり、６４－８＋３＝５９なので、元の２進数と同じ数を表現していることが分かる。ＮＡＦ変換では、出力のビット数は、最大で元のビット数＋１になることがあり、この例もそのようになっている。

[0047] 図７は図１のＮＡＦ変換装置をさらに別の例として具体化した４－ＮＡＦの変換装置である。図７に示すように、４－ＮＡＦの変換装置が有するＣは図１の構成における１ビット記憶手段４に対応する。同様に、Ｓ２とＳ１とＳ０は３ビットのシフトレジスタ３（ｗ＝４なのでｗ－１＝３ビット）に対応する。Ｙ３とＹ２とＹ１とＹ０は４ビットのパラレル出力に対応する。＋は１ビットの加算器であり、図１の更新手段２の要素である。

[0048] 図２の２－ＮＡＦ変換装置や図５の３－ＮＡＦ変換装置と図７の４－ＮＡＦ変換装置とを見比べてみると、シフトレジスタ３と出力が増えただけで同じ構造をもつことが分かる。

[0049] 図８を参照して、ｋを可変とするｋ－ＮＡＦ変換装置の例を示す。この例ではｋの値として２，３，４を選択できる。図８においてｋ－ＮＡＦ変換装置のＣは図１に示した構成における１ビット記憶手段４に対応する。Ｓ２と

Ｓ１とＳ０は図１の構成における３ビットのシフトレジスタ３（ｗ＝４なのでｗ－１＝３ビット）に対応する。Ｙ３とＹ２とＹ１とＹ０は４ビットのパラレル出力に対応する。＋は１ビットの加算器である。

[0050] Ｓはｋによって変わる最下位ビットである。ｋ＝２、つまりこの装置を２－ＮＡＦ変換装置として動作させるには、最下位ビットＳとしてＳ２を採用すればよく、同様に３－ＮＡＦ変換装置として動作させるためには、最下位ビットＳとしてＳ１を採用すればよく、４－ＮＡＦ変換装置の場合の最下位ビットはＳ＝Ｓ０とすればよい。このとき、出力は２－ＮＡＦのときはＹ３とＹ２とし、３－ＮＡＦのときはＹ３，Ｙ２，Ｙ１とし、４－ＮＡＦのときはＹ４，Ｙ３，Ｙ２，Ｙ１，Ｙ０とする。

[0051] 携帯機器のようにメモリが限られているような場面では、ｗを小さくすることで計算自体は遅くなるが、メモリを節約することができる。一般にｗを大きくすることで計算は速くなるがメモリ消費量が増える。例えばメモリの空きが少ないときはｗを小さくし、メモリの空きが多いときはｗを大きくすることで計算を速くすることができる。また、ｗを小さくし不要なレジスタへの給電を止めることで、電力を節約できる。

[0052] 図９を参照して、上述した２－ＮＡＦ変換装置を他の観点から説明する。すなわち、図９のような状態遷移表の形式で本実施形態に係る２－ＮＡＦ変換装置を説明する。図９において、ｓは今の状態（取りうる状態は３状態である）、ｉｎは１ビットの入力、ｓ’は次の状態、ｏｕｔは出力である。初期状態はｓ＝０である。入力ｉｎが１ビットずつ入るたびにｓとｉｎで決まるｓ’に状態遷移し、出力ｏｕｔを出力する。

[0053] 第１の状態において、入力が０のときは、第１の状態に状態遷移し、０を出力し、入力が１のときは、第２の状態に状態遷移し、０を出力する。第２の状態において、入力が０のときは、第１の状態に状態遷移し、１を出力し、入力が１のときは、第３の状態に状態遷移し、－１を出力する。第３の状態において、入力が０のときは、第２の状態に状態遷移し、０を出力し、入力が１のときは、第３の状態に状態遷移し、０を出力する。このようにして

整数の２進表現を下位から１ビットずつ入力すると２－ＮＡＦ表現された冗長２進表現を２ビットずつ出力する。

[0054] 図１０を参照して、２－ＮＡＦ変換装置をさらに説明する。図１０において、丸で囲まれているのが状態であり、状態遷移表のｓと対応する。３つの状態がある。数字／数字は、左の数字がｉｎ、右の数字がｏｕｔで、左の数字を入力したときに、右の数字を出力することを意味する。このような図１０は、図９の状態遷移表を状態遷移図の形に書き直したものである。初期状態は状態０である。

[0055] 図１１を参照して、上述した３－ＮＡＦ変換装置を他の観点から説明する。すなわち、図１１のような状態遷移表の形式に沿って本実施形態に係る３－ＮＡＦ変換装置を説明する。状態ｓとして取りうる値が０から４の５状態に増えており、出力は、３－ＮＡＦなので－３，－１，０，１，３の５通りになっている。

[0056] 第１の状態において、入力が０のときは、第１の状態に状態遷移し、０を出力し、入力が１のときは、第３の状態に状態遷移し、０を出力する。第２の状態において、入力が０のときは、第１の状態に状態遷移し、１を出力し、入力が１のときは、第５の状態に状態遷移し、－３を出力する。第３の状態において、入力が０のときは、第２の状態に状態遷移し、０を出力し、入力が１のときは、第４の状態に状態遷移し、０を出力する。第４の状態において、入力が０のときは、第１の状態に状態遷移し、３を出力し、入力が１のときは、第５の状態に状態遷移し、－１を出力する。第５の状態において、入力が０のときは、第３の状態に状態遷移し、０を出力し、入力が１のときは、第５の状態に状態遷移し、０を出力する。こうして、整数の２進表現を下位から１ビットずつ入力すると、３－ＮＡＦ表現された冗長２進表現を３ビットずつ出力する。

[0057] 図１２は、図１１の状態遷移表を状態遷移図に書き直したものであり、図１０と同様である。

[0058] 図１３を参照して、上述した４－ＮＡＦ変換装置を他の観点から説明する

。すなわち、図１３のような状態遷移表の形式に沿って本実施形態に係る４－ＮＡＦ変換装置を説明する。状態ｓとして取りうる値が０から８の９状態に増えている。出力は、４－ＮＡＦであので－７，－５，－３，－１，０，１，３，５，７の９種類である。

[0059] 第１の状態において、入力が０のときは、第１の状態に状態遷移し、０を出力し、入力が１のときは、第５の状態に状態遷移し、０を出力する。第２の状態において、入力が０のときは、第１の状態に状態遷移し、１を出力し、入力が１のときは、第９の状態に状態遷移し、－７を出力する。第３の状態において、入力が０のときは、第２の状態に状態遷移し、０を出力し、入力が１のときは、第６の状態に状態遷移し、０を出力する。第４の状態において、入力が０のときは、第１の状態に状態遷移し、３を出力し、入力が１のときは、第９の状態に状態遷移し、－５を出力する。第５の状態において、入力が０のときは、第３の状態に状態遷移し、０を出力し、入力が１のときは、第７の状態に状態遷移し、０を出力する。第６の状態において、入力が０のときは、第１の状態に状態遷移し、５を出力し、入力が１のときは、第９の状態に状態遷移し、－３を出力する。第７の状態において、入力が０のときは、第４の状態に状態遷移し、０を出力し、入力が１のときは、第８の状態に状態遷移し、０を出力する。第８の状態において、入力が０のときは、第１の状態に状態遷移し、７を出力し、入力が１のときは、第９の状態に状態遷移し、－１を出力する。第９の状態において、入力が０のときは、第５の状態に状態遷移し、０を出力し、入力が１のときは、第９の状態に状態遷移し、０を出力する。こうして整数の２進表現を下位から１ビットずつ入力すると４－ＮＡＦ表現された冗長２進表現を４ビットずつ出力する。

[0060] 図１４によって５－ＮＡＦ変換装置を示す。状態遷移表については図９の説明と同様である。状態ｓとして取りうる値が０から１６の１７状態に増えている。一般に、ｗ－ＮＡＦの場合は、２＾（ｗ－１）＋１状態を取る。

[0061] 上述した実施形態は順序回路によって実現できるが、同期回路としても非同期回路としても実現可能である。

[0062] サイドチャネル攻撃のような新たな暗号攻撃法が登場している。以上説明した実施形態によれば、楕円曲線暗号のスカラー倍の途中でｗを変化させることで、サイドチャネル攻撃を防ぐことが可能になる。ｗを変更できるのは、シフトレジスタが０の場合である。つまり、直前に０以外の値を出力したときである。

[0063] なお、本発明は上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施形態にわたる構成要素を適宜組み合わせてもよい。

符号の説明

[0064] １…受付手段；

２…更新手段；

３…ｗ－１ビットシフトレジスタ；

４…１ビット記憶手段

請求の範囲

[請求項1] 整数の２進表現をｗ－ＮＡＦ表現された冗長２進表現に変換するＮＡＦ変換装置であって、

前記整数の２進表現を下位から１ビットずつ受け付ける受付手段と、

１ビットで表現される状態の値を記憶する記憶手段と、

ｗ－１ビットで表現される状態の値を記憶するシフトレジスタと、

前記受付手段が受け付けた１ビットの値と、前記記憶手段の状態の値と、前記ｗ－１ビットのシフトレジスタの状態の値を参照し、次の時刻における前記記憶手段の状態と前記ｗ－１ビットのシフトレジスタの状態とを決定し、現時刻におけるｗビットのパラレル出力を決定する更新手段と、

を具備することを特徴とするＮＡＦ変換装置。

[請求項2] 前記更新手段は、

前記次の時刻における前記記憶手段の状態を、

前記現時刻における前記ｗ－１ビットのシフトレジスタの最下位ビットが１のときは、前記シリアル入力から入力された１ビットと前記現時刻の記憶手段の状態との和の下位１ビットとし、前記現時刻における前記ｗ－１ビットのシフトレジスタの最上位ビットが０のときは、前記和の上位１ビットとし、

前記次の時刻における前記ｗ－１ビットのシフトレジスタの状態を、

前記現時刻における前記ｗ－１ビットのシフトレジスタの最下位ビットが１のときは、ｗ－１ビットの０とし、前記現時刻における前記ｗ－１ビットのシフトレジスタの最下位ビットが０のときは、前記現時刻における該シフトレジスタを下位に向けて１ビットシフトし、該和の下位ビットを最上位ビットとしたｗ－１ビットの値とし、

前記現時刻におけるパラレル出力を、

前記和の下位ビットを最上位ビットとし、下位ｗ－１ビットが前記ｗ－１ビットのシフトレジスタの値とすることを特徴とする請求項１記載のＮＡＦ変換装置。

[請求項3] 前記ｗ－１シフトレジスタの最下位ビットに代えて、下位（ｗ－ｋ）ビットを使い、該パラレル出力の上位ｋビットを出力とすることを特徴とする請求項１記載のＮＡＦ変換装置。

[請求項4] ＣＰＵパワーおよびメモリ量を含む使用可能なリソースに応じた小さな値に前記ｋを設定することを特徴とする請求項３記載のＮＡＦ変換装置。

[請求項5] ＮＡＦ変換の途中でｋの値を２からｗの間で変化させることを特徴とする請求項３記載のＮＡＦ変換装置。

[請求項6] 前記１ビットの記憶手段、前記ｗ－１ビットのシフトレジスタ、前記更新手段が同期回路であることを特徴とする請求項１記載のＮＡＦ変換装置。

[請求項7] 前記１ビットの記憶手段、前記ｗ－１ビットのシフトレジスタ、前記更新手段が非同期回路であることを特徴とする請求項１記載のＮＡＦ変換装置。

[請求項8] １ビットシリアル入力と、

２ビットパラレル出力と、

３つの状態を記憶する記憶手段と、

第１の状態において、

入力が０のときは、第１の状態に状態遷移し、０を出力し、

入力が１のときは、第２の状態に状態遷移し、０を出力し、

第２の状態において、

入力が０のときは、第１の状態に状態遷移し、１を出力し、

入力が１のときは、第３の状態に状態遷移し、－１を出力し、

第３の状態において、

入力が０のときは、第２の状態に状態遷移し、０を出力し、

入力が１のときは、第３の状態に状態遷移し、０を出力する更新手段と、

を具備し、

整数の２進表現を下位から１ビットずつ前記シリアル入力から入力すると２－ＮＡＦ表現された冗長２進表現を２ビットずつ前記パラレル出力から出力する２－ＮＡＦ変換装置。

[請求項9] １ビットシリアル入力と、

３ビットパラレル出力と、

５つの状態を記憶する記憶手段と、

第１の状態において、

入力が０のときは、第１の状態に状態遷移し、０を出力し、

入力が１のときは、第３の状態に状態遷移し、０を出力し、

第２の状態において、

入力が０のときは、第１の状態に状態遷移し、１を出力し、

入力が１のときは、第５の状態に状態遷移し、－３を出力し、

第３の状態において、

入力が０のときは、第２の状態に状態遷移し、０を出力し、

入力が１のときは、第４の状態に状態遷移し、０を出力し、

第４の状態において、

入力が０のときは、第１の状態に状態遷移し、３を出力し、

入力が１のときは、第５の状態に状態遷移し、－１を出力し、

第５の状態において、

入力が０のときは、第３の状態に状態遷移し、０を出力し、

入力が１のときは、第５の状態に状態遷移し、０を出力する更新手段と、

を具備し、

整数の２進表現を下位から１ビットずつ前記シリアル入力から入力すると３－ＮＡＦ表現された冗長２進表現を３ビットずつ前記パラレ

ル出力から出力することを特徴とする３－ＮＡＦ変換装置。

[請求項10] １ビットシリアル入力と、

４ビットパラレル出力と、

９つの状態を記憶する記憶手段と、

第１の状態において、

入力が０のときは、第１の状態に状態遷移し、０を出力し、

入力が１のときは、第５の状態に状態遷移し、０を出力し、

第２の状態において、

入力が０のときは、第１の状態に状態遷移し、１を出力し、

入力が１のときは、第９の状態に状態遷移し、－７を出力し、

第３の状態において、

入力が０のときは、第２の状態に状態遷移し、０を出力し、

入力が１のときは、第６の状態に状態遷移し、０を出力し、

第４の状態において、

入力が０のときは、第１の状態に状態遷移し、３を出力し、

入力が１のときは、第９の状態に状態遷移し、－５を出力し、

第５の状態において、

入力が０のときは、第３の状態に状態遷移し、０を出力し、

入力が１のときは、第７の状態に状態遷移し、０を出力し、

第６の状態において、

入力が０のときは、第１の状態に状態遷移し、５を出力し、

入力が１のときは、第９の状態に状態遷移し、－３を出力し、

第７の状態において、

入力が０のときは、第４の状態に状態遷移し、０を出力し、

入力が１のときは、第８の状態に状態遷移し、０を出力し、

第８の状態において、

入力が０のときは、第１の状態に状態遷移し、７を出力し、

入力が１のときは、第９の状態に状態遷移し、－１を出力し、

第９の状態において、

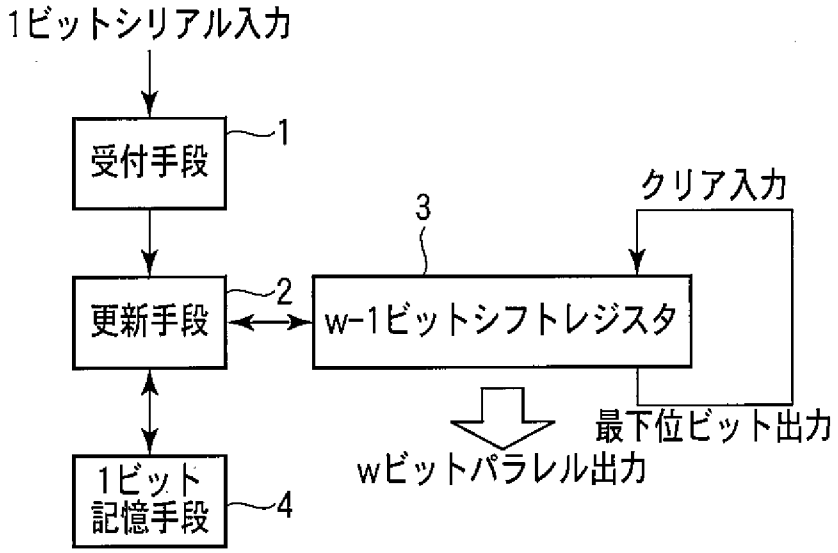
入力が０のときは、第５の状態に状態遷移し、０を出力し、

入力が１のときは、第９の状態に状態遷移し、０を出力する更新手段と、

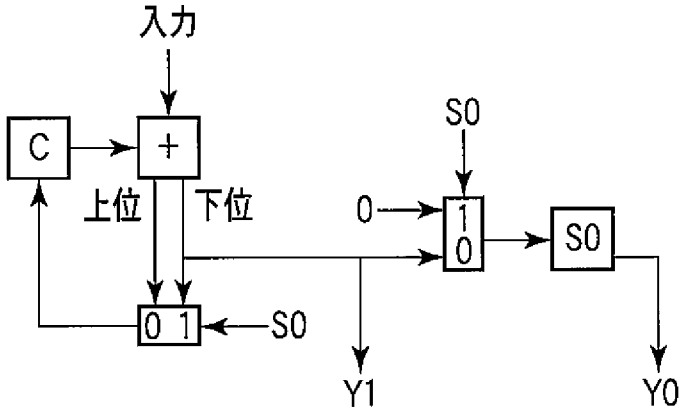
を具備し、

整数の２進表現を下位から１ビットずつ前記シリアル入力から入力すると、４－ＮＡＦ表現された冗長２進表現を４ビットずつ前記パラレル出力から出力することを特徴とする４－ＮＡＦ変換装置。

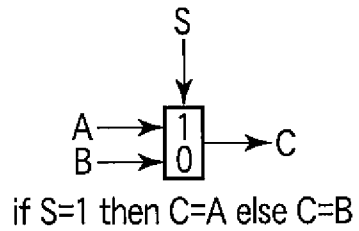
[図1]


1ビットシリアル入力
受付手段
1
更新手段
2
3
w-1ビットシフトレジスタ
クリア入力
最下位ビット出力
wビットパラレル出力
1ビット
記憶手段
4

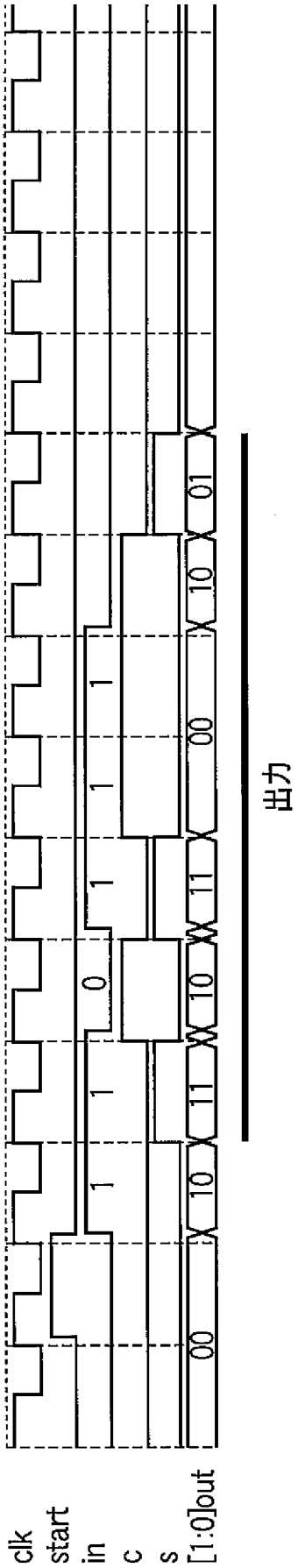
[図2]


入力
C
+
上位
下位
S0
0
1
0
S0
0 1
S0
Y1
Y0

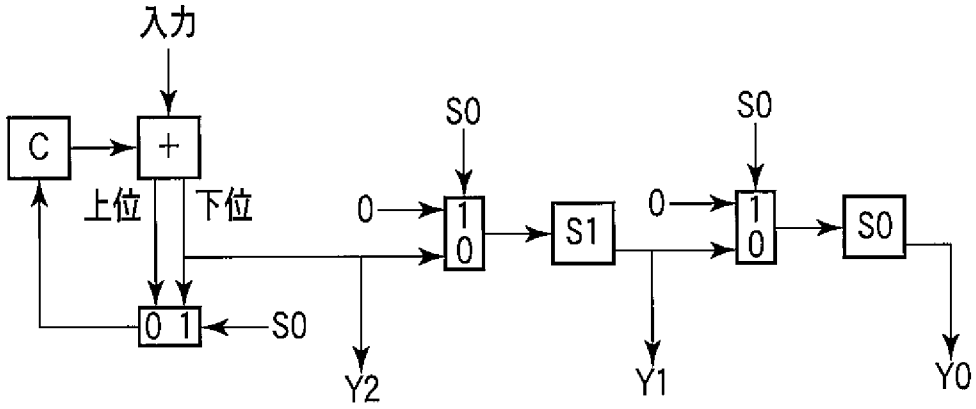
[図3]


S
A
B
1
0
C
if S=1 then C=A else C=B

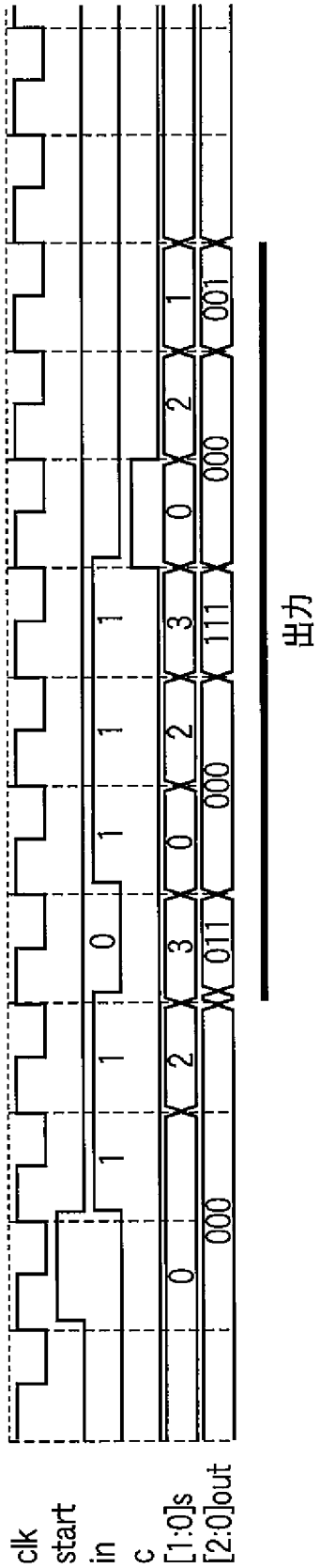
[図4]



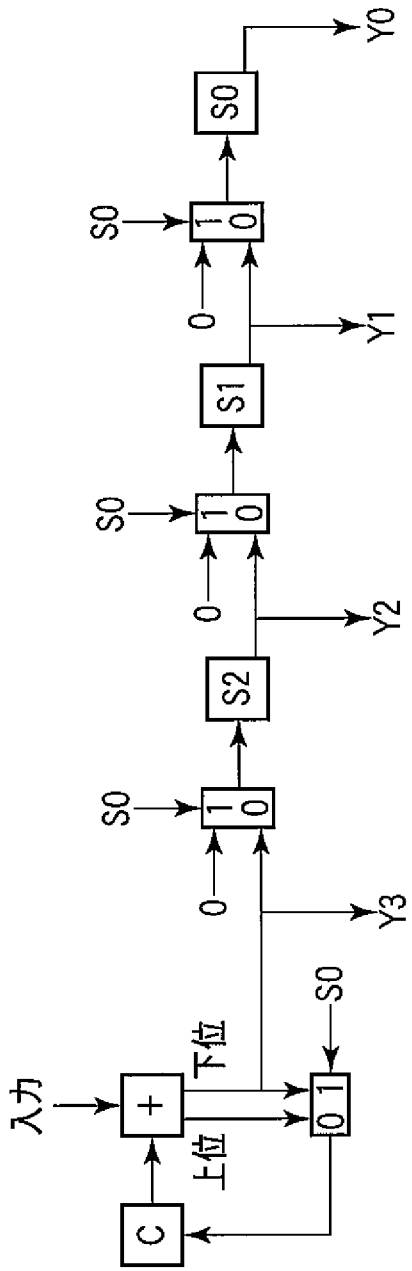
[図5]



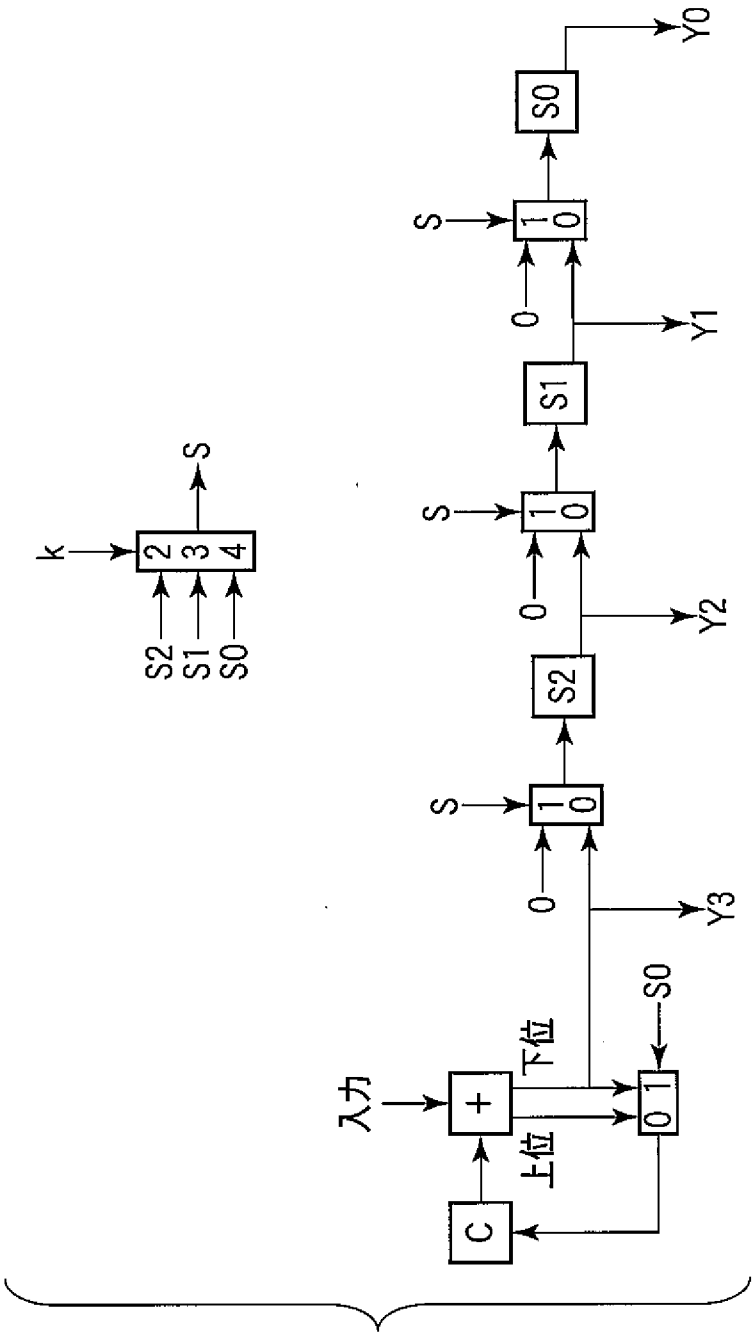
[図6]



[図7]



[図8]

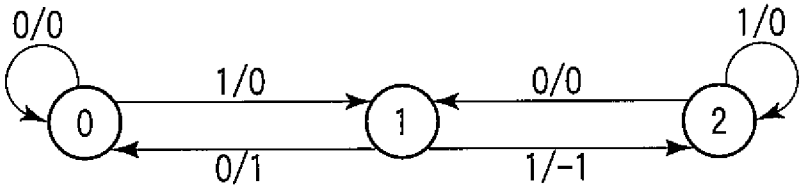


[図9]

s	in	s'	out
0	0	0	0
0	1	1	0
1	0	0	1
1	1	2	-1
2	0	1	0
2	1	2	0

s:今の状態　in:入力　s':次の状態　out:出力

[図10]

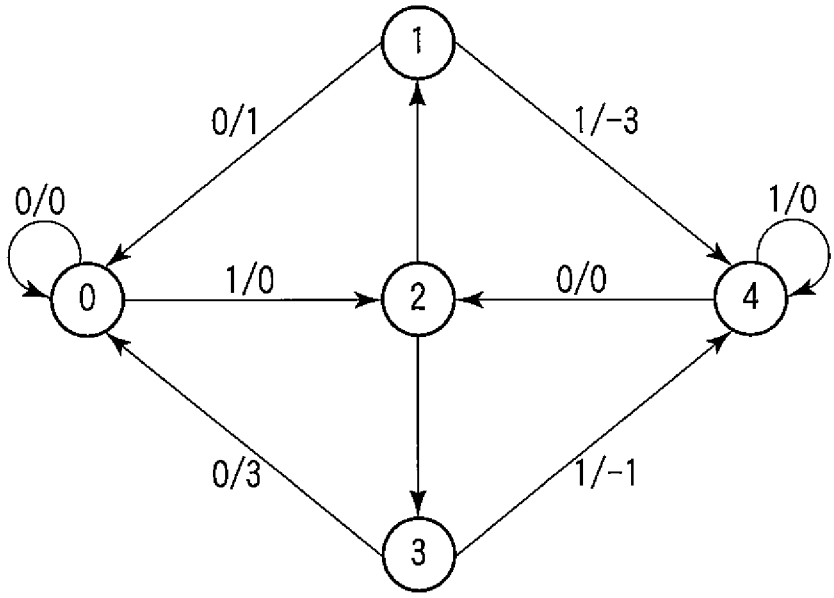


[図11]

s	in	s'	out
0	0	0	0
0	1	2	0
1	0	0	1
1	1	4	-3
2	0	1	0
2	1	3	0
3	0	0	3
3	1	4	-1
4	0	2	0
4	1	4	0

s:今の状態　in:入力　s':次の状態　out:出力

[図12]



[図13]

s	in	s'	out
0	0	0	0
0	1	4	0
1	0	0	1
1	1	8	-7
2	0	1	0
2	1	5	0
3	0	0	3
3	1	8	-5
4	0	2	0
4	1	6	0
5	0	0	5
5	1	8	-3
6	0	3	0
6	1	7	0
7	0	0	7
7	1	8	-1
8	0	4	0
8	1	8	0

s:今の状態　in:入力　s':次の状態　out:出力

[図14]

s	in	s'	out
0	0	0	0
0	1	8	0
1	0	0	1
1	1	16	-15
2	0	1	0
2	1	9	0
3	0	0	3
3	1	16	-13
4	0	2	0
4	1	10	0
5	0	0	5
5	1	16	-11
6	0	3	0
6	1	11	0
7	0	0	7
7	1	16	-9
8	0	4	0
8	1	12	0

s	in	s'	out
9	0	0	9
9	1	16	-7
10	0	5	0
10	1	13	0
11	0	0	11
11	1	16	-5
12	0	6	0
12	1	14	0
13	0	0	13
13	1	16	-3
14	0	7	0
14	1	15	0
15	0	0	15
15	1	16	-1
16	0	8	0
16	1	16	0

s:今の状態　in:入力　s':次の状態　out:出力

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2010/050420

A. CLASSIFICATION OF SUBJECT MATTER
H03M7/04(2006.01)i, *G06F7/49*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H03M7/04, G06F7/49

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2010
Kokai Jitsuyo Shinan Koho	1971-2010	Toroku Jitsuyo Shinan Koho	1994-2010

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	K.Okeya, T.Takagi, The Width-w NAF Method Provides Small Memory and Fast Elliptic Scalar Multiplications Secure against Side Channel Attacks, RSA conference cryptographer's track (CT-RSA 2003), 2003, LNCS 2612, p.328-343	8-10 1-7
X A	Marc Joye, Sung-Ming Yen, Optimal Left-to-Right Binary Signed-Digit Recoding, IEEE TRANSACTIONS ON COMPUTERS, 2000.07, VOL.49, NO.7, p.740-748	8 1-7,9,10
A	Tsuyoshi TKAGI, Sung-Ming YEN, Bo-Ching WU, Radix-r Non-Adjacent Form and Its Application to Pairing-Based Cryptosystem, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 2006.01, Vol.E89-A, No.1, p.115-123	1-10

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 15 March, 2010 (15.03.10)	Date of mailing of the international search report 23 March, 2010 (23.03.10)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2010/050420

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2006/054559 A1 (Sony Corp.), 26 May 2006 (26.05.2006), entire text; all drawings & JP 2006-145945 A & US 2007/0291937 A1 & EP 1816624 A1 & KR 10-2007-0085269 A & CN 101061526 A	1-10
A	JP 10-307705 A (Fujitsu Ltd.), 17 November 1998 (17.11.1998), entire text; all drawings & US 5986587 A	1-10
A	JP 63-311433 A (Nippon Telegraph And Telephone Corp.), 20 December 1988 (20.12.1988), entire text; all drawings (Family: none)	1-10
A	JP 1-226221 A (NEC Corp.), 08 September 1989 (08.09.1989), entire text; all drawings (Family: none)	1-10

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１０／０５０４２０

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H03M7/04(2006.01)i, G06F7/49(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H03M7/04, G06F7/49

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１０年
日本国実用新案登録公報	１９９６－２０１０年
日本国登録実用新案公報	１９９４－２０１０年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
X A	K. Okeya, T. Takagi, The Width-w NAF Method Provides Small Memory and Fast Elliptic Scalar Multiplications Secure against Side Channel Attacks, RSA conference cryptographer's track (CT-RSA 2003), 2003, LNCS 2612, p. 328-343	8-10 1-7
X A	Marc Joye, Sung-Ming Yen, Optimal Left-to-Right Binary Signed-Digit Recoding, IEEE TRANSACTIONS ON COMPUTERS, 2000.07, VOL. 49, NO. 7, p. 740-748	8 1-7, 9, 10

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１５．０３．２０１０	２３．０３．２０１０

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｋ　９２９７
北村　智彦
電話番号　０３－３５８１－１１０１　内線　３５５６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	Tsuyoshi TKAGI, Sung-Ming YEN, Bo-Ching WU, Radix-r Non-Adjacent Form and Its Application to Pairing-Based Cryptosystem, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 2006.01, Vol.E89-A, No.1, p.115-123	1-10
A	WO 2006/054559 A1（ソニー株式会社）2006.05.26, 全文, 全図 & JP 2006-145945 A & US 2007/0291937 A1 & EP 1816624 A1 & KR 10-2007-0085269 A & CN 101061526 A	1-10
A	JP 10-307705 A（富士通株式会社）1998.11.17, 全文, 全図 & US 5986587 A	1-10
A	JP 63-311433 A（日本電信電話株式会社）1988.12.20, 全文, 全図（ファミリーなし）	1-10
A	JP 1-226221 A（日本電気株式会社）1989.09.08, 全文, 全図（ファミリーなし）	1-10