SUOMI – FINLAND
(FI)

PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN

[A] TIIVISTELMÄ - SAMMANDRAG

(11) (21) Patenttihakemus - Patentansökan **20002152**

(51) Kv.lk.7 - Int.kl.7

G06F 12/14

(22) Hakemispäivä - Ansökningsdag **29.09.2000**

(24) Alkupäivä - Löpdag **29.09.2000**

(41) Tullut julkiseksi - Blivit offentlig **30.03.2002**

(71) Hakija - Sökande

1 •Setec Oy, Suometsäntie 1, 01740 Vantaa, SUOMI - FINLAND, (FI)

(72) Keksijä - Uppfinnare

1 •Paatero, Lauri, Rikalantie 4, 00970 Helsinki, SUOMI - FINLAND, (FI)

(74) Asiamies - Ombud: Kolster Oy Ab
Iso Roobertinkatu 23, 00120 Helsinki

(54) Keksinnön nimitys - Uppfinningens benämning

Menetelmä salaisen avaimen käsittelemiseksi
Förfarande för att hantera en hemlig nyckel

(57) Tiivistelmä - Sammandrag

Tämän keksinnön kohteena on laitteisto (1), joka käsittää: tulon (2) syötteen vastaanottamiseksi, lähdön (3) vasteen syöttämiseksi edelleen, ja laskinvälineitä (P), jotka vasteena tulon kautta vastaanotetulle syötteelle tuottavat vasteen ennalta määrättyä laskenta-algoritmia hyödyntämällä. Jotta salaisen avaimen käsittelystä ei vuotaisi ulkopuoliselle hyökkääjälle tietoja jotka auttavat salaisen avaimen selvittämistä käsittää laitteisto (1) muistin (M), johon on tallennettu salaisen avaimen osatekijöitä, jolloin mainittujen osatekijöiden summan vastaa salaisen avaimen arvoa, ja ainakin yksi mainituista osatekijöistä muodostuu toistensa kanssa kerrottavista luvuista, joista luvuista ainakin yksi luku on satunnaisluku, mainitun toistensa kanssa kerrottavista luvuista muodostuvan osatekijän ollessa tallennettuna muistiin erillisinä lukuina. Lisäksi laskinvälineet (P) on järjestetty hyödyntämään mainittuja mustiin (M) tallennettuja osatekijöitä vasteen laskemiseksi mainitulla laskenta-algoritmilla.

Uppfinningen avser en apparat (1), vilken omfattar: en ingång (2) för mottagning av en inmatningsstorhet, en utgång (3) för matning av ett svar vidare, samt beräkningsdon (P), vilka som svar på mottagningen av sagda inmatningsstorhet alstrar ett svar med hjälp av en beräkningsalgoritm. För att information beträffande behandlingen av en hemlig nyckel inte skall läcka ut till en utomstående angripare som kan hjälpa denne att klarlägga sagda hemliga nyckel, omfattar apparaturen (1) ett minne (M), i vilket har lagrats delfaktorer av sagda hemliga nyckel, varvid summan av sagda delfaktorer motsvarar värdet på sagda nyckel, och varvid minst en av sagda delfaktorer består av sinsemellan multiplicerade tal, av vilka minst ett tal utgöres av ett slumptal, varvid sagda av sinsemellan multiplicerade tal bildade delfaktor är lagrad i sagda minne i form av separata tal. Dessutom har sagda beräkningsdon (P) arrangerats att utnyttja sagda i minnet (M) lagrade delfaktorer, för beräkning av ett svar med hjälp av sagda beräkningsalgoritm.