United States District Court,
N.D. California, San Jose Division.

**CRYPTOGRAPHY RESEARCH, INC,**
Plaintiff.
v.
**VISA INTERNATIONAL SERVICE ASSOC., et al,**
Defendant.

No. C 04-04143 JW

**May 4, 2007.**

Darren E. Donnelly, J. David Hadden, Lynn Harold Pasahow, Erin Catherine Jones, Ryan Aftel Tyz, Saina Sason Shamilov, Fenwick & West, LLP, Stephen Roger Dartt, Mountain View, CA, David Douglas Schumann, Jedediah Wakefield, Fenwick & West, LLP, San Francisco, CA, Laurie Michelle Charrington, Day, Casebeer, Madrid & Batchelder, LLP, Cupertino, CA, for Plaintiff.

Brandon D. Baum, Eric Butler Evans, Michael A. Molano, Dennis S. Corgill, Ian N. Feinberg, John Joseph Fitzgerald, IV, W. Joseph Melnik, Mayer Brown, LLP, Palo Alto, CA, Elizabeth S. Campbell, Philadelphia, PA, Joshua Michael Masur, Fish & Richardson, PC, Redwood City, CA, Martin Frank Majestic, Hanson, Bridgett, Marcus, Vlahos & Rudy, LLP, Adam Paul Brezine, Esq., Jesse William Markham, Robert L. Stolebarger, Thomas McCarten Kerr, Holme, Roberts & Owen, LLP, Alexandra V. Atencio, Michael A. Duncheon, Hanson Bridgett, LLP, San Francisco, CA, Joseph Helmsen, Pittsburgh, PA, William Joseph Healey, Attorney at Law, Washington, DC, for Defendants.

## SECOND CLAIM CONSTRUCTION ORDER

JAMES WARE**, District Judge.**

## *I. INTRODUCTION*

This is an action brought by Plaintiff Cryptography Research, Inc .(CRI) against Defendant Visa International Service Association (Visa) for infringement of eight patents. The Court conducted claim construction proceedings on November 8-9, 2005. This is the Second Claim Construction Order in this case.

The background facts are stated in the Court's First Claim Construction Order. ( *See* Docket Item No. 269.) There are eight patents at issue in this case. This Order sets forth the Court's construction of the terms and phrases in the '783 Patent. This Order also modifies the Court's construction of claim language in the '661 Patent. ( *See* Docket Item No. 278.)

## *II. STANDARDS AND PROCEDURES FOR CLAIM CONSTRUCTION*

### **A.** ***General Principles of Claim Construction***

Claim construction is purely a matter of law, to be decided exclusively by the Court. Markman v. Westview Instruments, Inc., 517 U.S. 370, 387, 116 S.Ct. 1384, 134 L.Ed.2d 577 (1996). When the meanings of a word or phrase used in a claim is in dispute, the Court invites the parties to submit their respective proposed definitions and a brief, outlining the basis for their proposed construction. In addition, the Court conducts a hearing to allow oral argument of the respective proposed definitions. After the hearing, the Court takes the matter under submission, and issues an Order construing the meaning of the word or phrase. The Court's construction becomes legally operative meaning which governs further proceedings in the case. Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576, 1582 (Fed.Cir.1996).

**B.** ***Construction from the View Point of an Ordinarily Skilled Artisan***

An invention is defined by the language of the claim. Phillips v. AWH Corp., 415 F.3d 1303, 1322 (Fed.Cir.2005). In construing the meaning of claim language, the Court does so from the viewpoint of person of ordinary skill in art at the time of the invention. Thus, the Court seeks to construe the patent claim in accordance with what a person of ordinary skill in the art would understand the claim to mean at the time of the invention. The time of the invention is as of the effective filing date of the patent application. Id., at 1312.

The Court proceeds from an understanding that a person of ordinary skill in the art would come to an understanding of the meaning of the language of the claim by interpreting the language in the context of the intrinsic record. The instinsic record includes the language of the claim itself, and any surrounding claims, the written description, the drawings and the prosecution history-if they are in evidence. Teleflex, Inc. v. Fisosa N. Am. Corp., 299 F.3d 1313, 1324 (Fed.Cir.2002).

The Court approaches claim construction with an understanding that a person of ordinary skill in the art reading the intrinsic evidence would give consideration to whether the disputed word is one commonly used in lay language, a technical word or is a word coined by the inventor.

**C.** ***Commonly Used Words or Phrases***

If the disputed word or phrase is one which is commonly used in ordinary language, the Court considers that a person of ordinary skill in the art would give to it its ordinary and customary meaning, unless a specialized definition is stated in the patent specification or was stated by the inventor during prosecution of the patent. In articulating the ordinary and customary definition of a word which is commonly used in the English language, the Court may consult a general purpose dictionary. Phillips, 415 F.3d at 1314.

However, an inventor is free to act as his own lexicographer. Thus, acting as a lexicographer, the inventor may use a word or phrase differently than with its ordinary and customary meaning. Vitronics Corp., 90 F.3d at 1582. The Court examines the claim and other parts of the patent specification to determine if the inventor used the word with a specialized meaning.

A statement made by the inventor in the prosecution of the patent application as to the scope of the invention may be considered as evidence of what meaning to give to a word or phrase of a claim. Microsoft Corp. v. Multi-Tech Systems, Inc., 357 F.3d 1340, 1349 (2004). If it is in evidence, the Court examines the prosecution history of the patent for any specialized definition of a word or phrase used in a claim. A specialized definition clearly stated in the specification or during prosecution of a particular word or phrase is regarded by the Court as highly persuasive of the meaning of the word or phrase when it is used in a

claim. Phillips, 415 F.3d at 1322.

**D.** ***Technical Words or Phrases***

If the disputed word or phrase is a commonly used technical term in the field of the invention, the Court considers that one of skill in the art would give the word or phrase its ordinary and customary meaning in that technical field, unless a specialized definition is stated in the specification or was given to it during prosecution of the patent. In arriving at a definition, the Court may consult a technical art-specific dictionary or invite the parties to present testimony from experts in the field on the customary definition of the technical word or phrase. *Id*.

**E.** ***Coined Words or Phrases***

If the disputed word or phrase is coined by the inventor, the definition must be clearly stated in the patent documents. Vitronics Corp., 90 F.3d at 1582. If a definition of a coined word or phrase is not clearly stated or cannot be reasonably inferred, the Court may decline to construe the word pending further proceedings.

The Court recognizes that in the claim construction process, the Court is able to consider a number of extrinsic sources in any sequence it desires so long as it does not adopt a construction based on extrinsic evidence which contradicts the unambiguous meaning of a claim given in the intrinsic evidence. Phillips, 415 F.3d at 1324.

**F.** ***Declining to Construe a Word or Phrase***

If the Court is not able to come to a construction of any disputed word or phrase, the Court may decline to state a construction and may invite the parties to request a further hearing to address the matter.

**G.** ***Stipulated Meanings of Words or Phrases***

If the parties have agreed on the construction of a word or phrase and so stipulated in a statement to the Court, the Court may at any time re-construe the word or phrase, should it become clear that the intrinsic evidence does not support the agreed upon construction. If the intrinsic evidence does not explicitly define such words or phrases, the plain and ordinary meaning of such words or phrases as understood by someone skilled in the art would be used to determine if the agreed upon term is consistent with such understanding.

## *III. DISCUSSION*

### I. THE '661 PATENT

#### *The '661 Patent-Claim 1*

Claim 1 of the '661 Patent provides in part: FN1

A cryptographic processing device for securely performing a cryptographic processing operation including a sequence of instructions in a manner **resistant to** discovery of a secret by external monitoring, comprising ...

In its First Claim Construction Order, the Court construed the phrase "resistant to." CRI has requested the Court to reconsider its construction of this phrase. ( *See* Docket Item No. 271.) Visa contends that reconsideration is premature as the phase appears in other claims and patents which are awaiting the Court's construction; thus, Visa requests that the Court defers any reconstruction of the phrase until the entire claim construction process is completed. ( *See* Docket Item No. 272.)

The Court previously construed the phrase to mean: "less susceptible to external influence." Upon reconsideration, the Court finds that if its construction were to be substituted into Claim 1, it would produce a construction which would be redundant and confusing. Therefore, the Court vacates its previous construction in favor of the construction below.

Neither the patent specification nor the prosecution history state a specialized use of the phrase "resistant to." Thus, one of ordinary skill in the art would give the phrase "resistant to" its ordinary and customary meaning. The ordinary and customary meaning of "resistant to" is "offering resistance." However, to construe the phrase in this manner merely substitutes one form of the word "resist" for another, which the Court declines to do. Upon reconsideration, it appears to the Court that the dispute between the parties is whether the phrase should be construed to include a particular level of "resistance." In general, if a claim does not contain a limitation on the extent of a disclosed parameter, the Court should not add such a limitation. *See* Modine Manufacturing Co. v. U.S. International Trade Commission, 75 F.3d 1545, 1551 (Fed.Cir.1996). Previously, the Court concluded that the intrinsic evidence does not support limiting the phrase to a particular level. The Court reaffirms that conclusion.

The Court construes the phrase "**resistant to**" as it is used in Claim 1 of the '661 Patent as follows: The phrase "**resistant to**" requires no particular amount of resistance.FN2

**II. THE '783 PATENT**

**A. *The '783 Patent-Claim 6***

Claim 6 of the '783 Patent provides:

The method of claim 1 FN3 wherein **the probability that the value of any specific bit in any of said randomized quantities is a "one" is one half (0.5).**

The parties dispute the construction of the emphasized phrase. The dispute is whether the phrase should be construed to require that the probability be " *exactly* " one half.

Claim 6 uses the word "probability." The request that the Court include the word "exactly" in its construction of Claim 6 apparently proceeds from probability theory. One of ordinary skill in the art would understand that the inventor intended the word "probability" to have its ordinary and customary meaning, namely, a mathematical expression of the frequency with which a event is likely to occur.

The requested construction is also apparently based on the probable value of a specific "bit." A "bit" is a contraction of the phrase "binary digit." Application of John P. Mahony, 57 C.C.P.A. 939, 421 F.2d 742 (C.C.P.A.1970). "[In] computers bits appear in the physical form of pulses or the absence of pulses, and that the present or absence of a pulse is in turn represented by the characters 1 and 0." Id. at 746. Thus under probability theory, if an equally weighted two-sided coin is flipped, at the commencement of the flip, the probability that the coin will land heads-up or tails-up is 1 in 2 or, equivalently fifty percent. The requested

construction is apparently based on the reasoning that since a bit is either a "one" or a "zero," if a method requires that the probability that a particular bit be a "one," is 0.5, then the probability of it being a zero must be exactly 0.5. The conclusion that the Court is asked to adopt is that if the probability were higher or lower than exactly 0.5, the method would not be practiced.

The language of Claim 6 does not contain a limitation that the probability must be "exactly" 0.5. There is a discussion in the written description of an embodiment of a method in which the term "exactly 0.5" is used:

In this embodiment, the permutations and blinded values can be produced as follows. * * * Although not necessary to the present invention, the exemplary embodiment has the properties that: (a) for any key, H(K1) and H(K2) average to 64/2=32, where H(X) is the Hamming Weight of X, (b) the probability that any specific bit in either K1 or K2 is a 1 **is 0.5,** and (c) correlations between register locations and key bits are weak (or equal to **exactly 0.5) .** These properties can reduce the amount of useful information leaked by the system to an attacker.

('783 Patent, Col. 6:39-63.) However, the Court declines to read the limitations of an embodiment into the claim. Moreover, the method is not limited to a random number process for assignment of a value of "one" or "zero" to a particular bit. The inventors of the '783 patents defined "random" to include "pseudorandom" FN4 values, which skew the results from a strictly random probability process.

The Court declines to include "exactly" in a construction of Claim 6. Since this is the only dispute with respect to Claim 6, the Court declines to give further consideration to Claim 6 at this time.

**B. *The '783 Patent-Claim 13***

Claim 13 of the '783 Patent provides:

The method of claim 1 further comprising:

* * *

(d) **updating at least one of said randomized quantities** using additional unpredictable information to generate at least one updated randomized quantity; and

* * *

The parties dispute the proper construction of the phrase "updating at least one of said randomized quantities." The word "updating" is discussed in several sections of the specification. The "Summary of the Invention" provides:

This invention describes processes in which secrets (e.g., keys and/or messages) are divided into separate portions, which are then separately mutated, while maintaining mathematical relationships between or among the portions that are used for performing secure cryptographic operations. **In the update ("mutation") operation, key management devices introduce randomness or other unpredictability into their internal state.** By changing the secret portions, information collected by attackers about them can be made obsolete. If information is invalidated faster than it can be collected by attackers, a system can be made secure.

('783 Patent, Col. 1:66-2:9.)

The process of "updating" is also discussed with respect to an embodiment of the invention:

For greater security, during operation of the device **the tables are preferably periodically updated** so that attackers will not be able to obtain the table contents by analysis of measurements. The **updating process** should preferably introduce fresh entropy into the tables faster than information leaks out. Such an **update process** can require a significant amount of time, particularly if the S tables are stored in memory such as some EEPROM that is slow to update. To prevent the **update process** from introducing unpredictable processing delays, the **update** can occur gradually, so that a portion of the S table is **updated** at a time. Idle time, if available, can also be used for **table updates.**

('783 Patent, Col. 8:6-17.)

One of ordinary skill in the art would understand that the inventors of the ' 783 patent are using the word "updating" to describe a process of changing a value in some fashion so that an attack based on the old value is frustrated. Thus, the limitations on "updating" as disclosed in Claim 13 are that it be performed on "at least one of the randomized quantities" disclosed in Claim 1, and that the method be performed "using additional unpredictable information."

Further, the "updating" step of Claim 13 is broader than the step disclosed in dependent claims 14 and 15, which disclose updating by "reordering" and "randomizing," respectively. Therefore, the Court will not limit its construction of "updating" to these two methods.

The Court construes the phrase, "**updating at least one of said randomized quantities**" in Claim 13 to mean: **changing at least one of said randomized quantities.**

**C.** ***The '783 Patent-Claim 17***

Claim 17 of the '783 Patent provides:

The method of claim 13 wherein step (c) includes performing said first step of said operation using a plurality of parameters, said method further comprises using said initial unpredictable information to initialize said parameters and updating said parameters to generate a plurality of updated parameters, and step (e) includes performing said second step of said operation using said updated parameters.

The only dispute with respect to Claim 17 is whether the method should be construed to be limited to an algorithm called Data Encryption Standard or "DES."

The Summary of the Invention states:

The invention provides for improved implementations of the **Data Encryption Standard (DES), as well as other cryptographic operations,** that resist external monitoring attacks. **Unlike traditional DES implementations,** which perform a set of processing operations that depend only on the input key and the message, **the invention involves additional random (or otherwise unpredictable) state information in the cryptographic processing.** The random state information is mixed with the keys, plaintext messages,

and intermediate quantities used during processing. Information leaked to attackers during cryptographic processing is correlated to the random information, and any correlation to secret information is partially or completely hidden. As a result, it is difficult or impossible for attackers to determine secret parameters through analysis of leaked information.

('783 Patent, Col. 2:10-24.)

One skilled in the art would understand that the inventors of the '783 patent are not limiting any of the claims to DES. Even the claims which explicitly refer to DES, disclose a method "compatible with" DES. For example Claim 8 provides:

The method of claim 1 wherein said cryptographic operation is **compatible with** the Data Encryption Standard **(DES),** said method further comprising recombining the result of step (c) to produce a final result, said final result being a cryptographic representation of said message transformed with said **DES** algorithm.

The Court finds that a claim "compatible with" DES is not limited to DES. Thus, neither Claim 8 nor Claim 1 from which it depends is limited to DES.

In addition, the lack of any limitation of any of the claims to DES is further confirmed by the '783 patent's summary which states:

... although the invention has been described with respect to DES, the invention can be applied to and adapted to other cryptographic symmetric algorithms, including without limitation Blowfish, SEAL, IDEA, SHA RC5, TEA and other cryptographic algorithms involving operations suitable for application of the techniques of the invention.

('783 Patent, Col. 3:14-20.)

The Court construes Claim 17 as follows: **Claim 17 is not limited to DES.** FN5

**D.** ***The '783 Patent-Claim 18***

Claim 18 of the '783 Patent provides:

A method for performing a cryptographic operation on a message using a key, comprising:

(a) using unpredictable information, transforming said message into a plurality of message portions having a predetermined logical relationship thereamong;

(b) using unpredictable information, transforming said key into a plurality of key portions having a predetermined logical relationship thereamong;

(c) performing a first step of said cryptographic operation on said message portions using said key portions in a hardware device to reduce the amount of useful information about said operation available from external monitoring of said hardware device;

(d) updating at least one of said plurality of message portions with unpredictable information;

(e) updating at least one of said plurality of key portions with unpredictable information;

(f) **performing at least a second step of said cryptographic operation on said message portions** using said key portions in a hardware device to reduce the amount of useful information about said operation available from external monitoring of said hardware device; and

(g) returning a cryptographic result.

The parties dispute the construction of the phrase, "performing at least a second step of said cryptographic operation on said message portions using said key portions." The dispute is whether the "second step" is performed on updated information or on information which has not been updated.

Claim 18 is a method claim. Unless the steps of a method actually recite an order, ordinarily the steps should not construed to require one. Altiris, Inc., v. Symantec Corp., 318 F.3d 1363, 1369 (Fed.Cir.2003). Claim 18 discloses a "method ... comprising ... a first step of said cryptographic operation on said message portions using said key portions" FN6 and "at least a second step of said cryptographic operation." FN7 Although the phrases "first step" and "second step" are used to describe "step (c) and "step (f)," the method contains steps before the "first step" and intervening steps before the "second step." One of skill in the art would understand from reading the patent claims and specifications that the inventors of the '783 patent did not use the phrase "first step" to mean the first step of the method. There are two steps in the method which precede "step (c)," namely, "transforming" the message into "a plurality of message portions" and "transforming" the key "into a plurality of key portions." One of skill in the art would understand the phrases, "first step" and "second step" as referring to particular points in the overall process.

Further, the Preamble of Claim 18 discloses a "cryptographic operation" on "a message using a key." Step (a) transforms "said message" into a plurality of "message portions." Step (b) transforms "said key" into a plurality of "key portions." Step (c) performs a first encryption on "said message portions" using "said key portions." Step (d) updates "at least one of said plurality of message portions." Step (e) updates "at least one of said plurality of key portions." Step (f) performs "at least" a second encryption on "said message portions using said key portions ." Based on the language of the claim, steps (a) through (f) are antecedent to each succeeding step. Thus, one of skill in the art would understand that "step (f)" is performed on the message portions, at least one of which had been updated in step (d) with the key portions, at least one of which was updated in step (e). To construe the claim otherwise would be to render steps (d) and (e) superfluous.

In addition, the Court has construed the phrase "updating" a value as "changing" that value. There is no disclosure in the Claim or anywhere else in the specification of a separation of the updated message portion from the rest of the "said message portions ." Consequently, once a change is made in performing the "updating" step, the initial "message portions" and initial "key portions" no longer exist. Hence the "step (f)" could not be performed on pre-updated portions.

The Court notes that although in Figure 1, an embodiment of the invention shows a loop back from a round of encryption (155) to the updating step (135), Claim 18 does not disclose a loop back from step (f) to any previous step. FN8 Thus, the "at least a second step" must be performed. The phrase "at least a second step" means that there could be a third or optionally additional rounds of encryption. However, because the method does not disclose a loop back to any particular point, any third or succeeding encryption must be performed on the data returned from step (f) without further updating from the performance of steps (d) and

(e).

The Court construes the phrase, "**performing at least a second step of said cryptographic operation on said message portions using said key portions**" in Claim 18 to mean: **performing at least a second round of encryption on the updated message portions using the updated key portions.**

**E.** ***The '783 Patent-Claim 24***

Claim 24 of the '783 Patent provides:

The device of claim 22 wherein said power consumption varies measurably during said cryptographic transformations, but **where measurements of said power consumption are not correlated to said secret quantity.**

The parties dispute the construction of the phrase, "where measurements of said power consumption are not correlated to said secret quantity."

As an initial matter, the Court notes that Claim 24 discloses that the " *measurements* of the power consumption are not correlated" to the secret quantity. The word "measurement" is commonly used to refer to the act of measuring and the result from measuring. The Court construes the phrase "measurements are not correlated" to disclose a device with no correlation between the result from measuring, i.e., "power consumption" and the secret quantity as opposed to a device with no correlation between the act of measuring the power consumption and the secret quantity.

Claim 24 depends from Claim 22. The phrase "said power consumption" in Claim 24 refers to the power consumption of the "cryptographic processing device," which is disclosed in Claim 22. The dispute is over the phrase "not correlated to said secret quantity." The concept of "correlation" or lack of correlation is first introduced in the "Background of the Invention" section of the specification:

The invention provides for improved implementations of the Data Encryption Standard (DES), as well as other cryptographic operations, that resist external monitoring attacks. Unlike traditional DES implementations, which perform a set of processing operations that depend only on the input key and the message, the invention involves additional random (or otherwise unpredictable) state information in the cryptographic processing. The random state information is mixed with the keys, plaintext messages, and intermediate quantities used during processing. Information leaked to attackers during cryptographic processing is **correlated** to the random information, and **any correlation to secret information is partially or completely hidden.** As a result, it is difficult or impossible for attackers to determine secret parameters through analysis of leaked information.

('783 Patent, Col. 10:10-24.)

In the written description, the inventors of the '783 patent discuss how correlation between power consumption and the secret key can be used to facilitate an unauthorized detection of the secret key in data manipulation operations:

Data manipulation operations reveal information about the data being processed. For example, the power consumption of a typical operation (whether in a microprocessor or gate-level hardware implementation of

DES) is **correlated** to the data being manipulated. For example, shifting a byte with a Hamming weight of 5 will take a significantly different amount of power than shifting a byte of Hamming weight 4. Another example: power consumption is **correlated** to values on the address bus (such as addresses of bytes fetched for S table lookups), revealing information about the internal processing of the DES algorithm. An attacker can verify guesses about key bits by checking whether expected biases or effects appear in collected data.

('783 Patent, Col. 5:16-29.)

Weakening the correlation between power consumption and other operations are discussed as a way of protecting the secret key:

(d) Table lookup operations leak information about the address of the memory lookup and the value that is returned.

* * *

(e) Operations that change the device state (including the memory contents, processor flags, registers, etc.) can reveal information about the initial and final states of the operation.

* * *

(f) Variations between individual transistors in an integrated circuit, variations in the electrical properties of wires within a chip, variations in the amount of electromagnetic radiation emitted by different wires, etc. can all provide variations detectable by an attacker that can be analyzed statistically to determine secret keys.

* * *

In one embodiment of the invention, the inputs to the DES function (the plaintext and the key, when encrypting) are encoded in a different form than usual. Standard DES implementations use a 56-bit key K (commonly stored as 8 bytes with an ignored parity bit in each byte) and a 64-bit plaintext message M. However, the process of loading a key or message into a standard DES implementation can leak information about the key or plaintext.

Thus, a preferred improved DES implementation of the invention instead uses two 56-bit keys (K1 and K2) and two 64-bit plaintext messages.

* * *

In this embodiment, the permutations and blinded values can be produced as follows.

* * *

Although not necessary to the present invention, the exemplary embodiment has the properties that: (a) for any key, H(K1) and H(K2) average to 64/2=32, where H(X) is the Hamming Weight of X, (b) the probability that any specific bit in either K1 or K2 is a 1 is 0.5, and (c) **correlations** between register locations and key bits are weak (or equal to exactly 0.5). These properties can reduce the amount of useful information leaked by the system to an attacker.

At the end of such operations, the two parts of the ciphertext may be recombined to form the same encrypted/decrypted quantity that would have been produced by a standard DES protocol.

('783 Patent, Col. 5:30; Col.6-67.)

One of skill in the art would understand that the "correlation" the inventors of the '783 patent are concerned about is between power consumption and a process being carried out by the device. In some Claims of the '783 Patent, the correlation is claimed to be "undetectably small" or "measurably significant." Claim 26 provides:

The device of claim 22 further comprising at least one register for temporarily storing said randomized quantities, wherein **the correlation** between any single bit of said at least one register and said secret quantity **is undetectably small,** but where **the correlation** between a combination of multiple bits of said at least one register and said secret quantity **is measurably significant.**

Claim 34 discloses a device in which there is "no measureable correlation" between parameters:

The device of claim 33 where said key processing unit is further configured to derive a plurality of parameters from said secret parameter and said blinding value such that a mathematical relationship exists between said derived plurality of parameters and said obtained secret parameter, but where **no measureable correlation** is present between any one of said pluarlity of parameters and said secert [sic] parameter.

Thus, when Claim 24 uses the phrase "not correlated," one of skill in the art would understand that the Claim limitation "no correlation" is different from a Claim limitation of a correlation which is "measurably significant," or "weak," or "undetectably small."

The Court construes the phrase "**where measurements of said power consumption are not correlated to said secret quantity**" to mean: **where there is no correlation between power consumption and the secret quantity during cryptographic operations.**

**G.** ***The '783 Patent-Claim 28***

Claim 28 of the '783 Patent provides:

A method for performing a symmetric cryptograhic operation using a secret key with resistance to external monitoring attacks, comprising:

(a) obtaining an input message;

(b) generating initial unpredictable information;

(c) combining said key, said message, and said unpredictable information;

(d) **deriving a result,** where:

**(i)said result is a predefined function of said input message and of said key, and**

**(ii) said result is independent of said unpredictable information; and**

(e) producing a response based on said result.

The parties dispute the proper construction of the highlighted steps. Claim 28 is a method for performing a symmetric cryptographic operation comprising 5 steps:

(1) The first step is "obtaining an input message." The "input message" is a digital quantity.FN9

(2) The second step is "generating initial unpredictable information." The unpredictable information" would be in the form of a digital quantity. FN10

(3) The third step is "combining said key, said message, and said unpredictable information." The "key" is the "secret key" in the Preamble. The "secret key" is a digital quantity or is converted to one as part of the process.FN11 Neither Claim 28 nor the specification disclose how the key, message and unpredictable information are "combined." Since the next step refers to "said input message" and "said key," the combination must be done in a way to allow the method to operated on the input message and the key even after they have been "combined."

(4) The fourth step, and the step in dispute is: "deriving a result, where: (i) said result is a predefined function of said input message and of said key, and (ii) said result is independent of said unpredictable information. The phrase "deriving a result," would be understood by a person of ordinary skill in the art as producing a mathematical result from a mathematical operation.

Claim 28 discloses that the mathematical "result" would be a predefined "function" of two quantities: the digital input message and the digital secret key. One of ordinary skill in the art would understand the word "function" as a mathematical term meaning a way to associate an output for specified inputs. A function can be represented in many ways, among them: a formula or algorithm. Claim 28 does not disclose what "predefined function" is used.

Claim 28 discloses limitations on the "result:" First, Claim 28 discloses that the function uses two quantities: the digital input message and the digital secret key. One of ordinary skill in the art would understand "independent" in is plain ordinary meaning, namely, "does not depend on." The "combination" disclosed in step (3) and the "deriving a result" disclosed in step (4) must be performed in a manner which combines the unpredictable information in a manner in which does not allow it to affect the "result."

(5) The fifth step is "producing a response based on said result." One of skill in the art would understand the "response" may be different from the "result."

The Court construes "**deriving a result, where: (i) said result is a predefined function of said input message and of said key, and (ii) said result is independent of said unpredictable information" to mean: producing a result which is based on a function of the key and the message, which are in combination with unpredictable information. The unpredictable information is combined in a manner which obscures the key and other information but which does not change the result.**

**H.** ***The '783 Patent-Claim 37***

Claim 37 of the '783 Patent provides:

**A method for reducing the correlation between physical attributes of a cryptographic system** and the values of secret parameters being manipulated during a cryptographic operations, by masking a table lookup operation, consisting of the following steps:

(a) **receiving a representation of a lookup table for use in said table lookup operation;**

(b) receiving input and output **masking parameters** corresponding to said received table representation;

(c) obtaining some unpredictable information;

(d) deriving a transformed representation of said lookup table from said received lookup table and said unpredictable information;

(e) deriving new input and output masking parameters corresponding to said transformed representation of said table;

(f) storing said transformed lookup table and said input and output masking parameters in a memory; and

(g) using said transformed table in a cryptographic computation.

The parties dispute the construction of the four emphasized phrases.

**1. "a method for reducing the correlation"**

The parties dispute whether the phrase "reducing the correlation" should be construed to include a level of reduction. Consistent with its discussion with respect to Claim 1 of the '661 Patent, the Court declines to add any amount of reduction to Claim 37.

**2. "physical attributes of a cryptographic system"**

The parties submit common definitions of the phrase "physical attributes of a cryptographic system," namely, power consumption and electromagnetic radiation. The Court declines to adopt this construction even though the parties have stipulated to the definition.

Although Claim 37 is a method claim, the phrase "cryptographic system" refers to a device. The written description discusses power consumption electromagnetic radiation as attributes of the device which make the process vulnerable to attack:

For physically large systems, effective physical shielding, physical isolation, and careful filtering of inputs and outputs are known in the background art (e.g., U.S. government Tempest specifications). Such shielding techniques can protect cryptographic devices from external monitoring attacks that involve analyzing **power consumption, electromagnetic radiation** (both in air and coupled to the device's inputs and outputs), electrical activity within the device, etc. as well as protecting against physical attacks. Unfortunately, these techniques are difficult to apply in constrained engineering environments. For example, physical constraints (such as size and weight), cost requirements, and the need to conserve power can often prevent the use of

previously-known.

('783 Patent, Col. 2:32-45.)

The specification does not limit the physical attributes of the cryptographic system to power consumption and electromagnetic radiation. Power consumption is listed as an example of a physical attribute of the process:

In a common situation, an attacker monitors a physical property, **such as power consumption,** of a secure token as it performs a cryptographic operation.

('783 Patent, Col. 3:43-45.)

One skilled in the art would understand that the inventors of the '783 Patent use the phrase "physical attributes according to its widely accepted meaning, namely, "attributes which follow the laws of physics." Physical phenomena can be measured. Although the parties are correct that power consumption and electromagnetic radiation are two measurable physical attributes of the process, the specification does not limit the claim language to those two attributes. For example, the specification discusses "electrical activity within the device." Such activity may be a different attribute from power consumption. The Court declines to limit the phrase "physical attributes" to a particular attribute.

The Court construes the phrase "**physical attributes of the cryptographic system**" to mean: **the properties of a cryptographic system produced during the performance of the cryptographic process which are measurable.**

**3. "receiving a representation of a lookup table for use in said table lookup operation"**

The parties dispute the proper construction of the phrase "lookup table." The Court is asked to construe the phrase to mean a "substitution table." A common expression for a substitution table is "S table." The written description contains references to the phrases "S table lookup operations" and "table look up operations:"

Finally, **for the S table lookup operations,** the S tables themselves are stored in the device's memory in blinded form, such that the S table inputs and outputs are blinded with random values.

* * *

**Table lookup operations** leak information about the address of the memory lookup and the value that is returned. Particularly serious sources of such leakage include the device's power consumption and electromagnetic radiation.

('783 Patent, Col. 2:63-66; Col. 5:30-35.)

Many of the references in the specification are to "S table lookup operations" which are used as part of the DES.

The standard DES algorithm involves three primary types of operations: permutations, **S lookups,** and bitwise XORs. In the exemplary embodiment, permutations of the message (M1, M2, M1P, M2P) are

performed by manipulating M1P and M2P.

('783 Patent, Col. 2:44-48.)

The phrase "lookup table" has a plain customary meaning to those skilled in the art, namely, a table of values used in obtaining the value of a function using a table look-up procedure. *See Institute of Electrical and Electronics Engineering (IEEE) Dictionary of Standards Terms,* p. 640 (7th Ed.2000). Accordingly, the Court declines to construe the phrase "lookup table" as limited to a substitution table. The Court finds that the phrase does not require construction.

**4. "masking parameters"**

The parties dispute the proper construction of the phrase "masking parameters."

The words "mask" and "unmask" are used in the written description and in the claims of the to describe various processes which conceal input and output values:

Many variations and adaptations of the invention are possible. For example, the message bits can be stored in 128-bit arrays where the bits are intermingled (as opposed to having separated halves), keys can be manipulated in 64-bit form instead of 56-bit form, orderings can be reversed or permuted (including in ways that do not change the final result of the computation). Rather than blinding operations with XOR halves, other bit operations can be applied. Where basic operations other than XOR bit operations are used, other splitting and/or blinding functions can be used. To save memory, permutation tables can be eliminated while maintaining randomness in table orders by encoding tables such that XORing with a **mask** (or applying another index **unmasking** function) yields the final pointer to the data.

('783 Patent, Col. 13:8-21.)

The Court construes the phrase "**masking parameters**" to mean: **values used to conceal another value.**

**I. *The '783 Patent-Claim 38***

Claim 38 of the '783 Patent provides:

The method of claim 37 where step (d) includes the following substeps:

(d1) obtaining a first random value;

(d2) generating a new output masking value from said first random value and an output masking value received at step (b);

(d3) obtaining a second random value;

(d4) generating a new input masking value from said second random value and an input masking value received at step (b);

(d5) producing said transformed table with the property that the ith element in the transformed table is equal to the result of

(i) finding the element at the location in the original table specified by taking an index 'i' XORed with said old input mask,

(ii) XORing said element with the values of both said new output mask and said old output mask,

(iii) storing said XOR result in said transformed table at a location corresponding to said index 'i' XORed with said new input mask.

The parties request the Court to find whether Claim 38 is valid or invalid on the ground that it is a dependent claim which impermissibly adds new steps. The dispute grows out of the fact that Claim 38 depends from Claim 37. Claim 37 uses the phrase "consists of" to describe its recited elements. Ordinarily, a claim which depends from a claim which "consists of" recited elements or steps cannot add an element or step. *Manual of Patent Examining Procedures* s. 2111.03 (8th Ed., Rev.2, 2004.)

The Court finds that Claim 38 does not add a new step to Claim 37, it merely limits step (d) of Claim 37. Therefore, the Court finds no basis for declaring Claim 38 invalid for impermissible claiming.

## *IV. CONCLUSION*

In this Order, the Court has construed some of the disputed words and phrases of the '783 Patent submitted for construction. There were words and phrases submitted for construction which were not addressed in this Order. To the extent a party believes that further claim construction is necessary, the Court invites that party to submit a request to that effect.

FN1. Unless otherwise indicated, all bold typeface is added by the Court to emphasize words and phrases under consideration.

FN2. This construction also applies to the phrase "resistant to" as it is used in Claims 6, 9, 11, 15, 26, 27, and 29 of the '661 Patent; Claims 22 and 28 of the '783 Patent; and Claims 1, 13, 18, and 31 of the ' 442 Patent; Claim 39 of the '658 Patent; Claims 2, 11, and 31 of the '518 Patent; and Claim 1 of the '884 Patent.

FN3. Claim 6 depends from Claim 1. Claim 1 provides:
A method for performing a cryptographic operation on a message, comprising:

(a) generating initial unpredictable information;

(b) using said initial unpredictable information, transforming an initial secret quantity into a plurality of randomized quantities having a predetermined logical relationship thereamong; and

(c) performing a first step of said operation involving said randomized quantities in a hardware device to reduce the amount of useful information about said operation available from external monitoring of said hardware device.

FN4. In a discussion of a preferred embodiment, the inventors of the '783 patent defines the word "random:" As used herein, the term "random" shall include truly random values, as well as pseudorandom and other values that are unpredictable by an attacker. ('783 Patent, Col. 6:42-45.) Thus, the Court construes the word "random" to include pseudorandum values.

FN5. There are other instances in which a party contends that a method claim of the '783 patent should be construed in a manner which would limit it to DES. See e.g., the contentions of the parties with respect to Claim 33. The Court's construction that Claim 17 is not limited to DES applies to all of the Claims of the '783 Patent, unless the Court specifically finds otherwise.

FN6. For clarity of reference, this step will be referred to as "step (c)."

FN7. For clarity of reference, this step will be referred to as "step (f)."

FN8. In contrast, for example, Claim 4 of the '442 Patent discloses a loop back from step (g) back to steps (d) through (g).

FN9. A detailed description of how the invention may be applied to the Data Encryption Standard is provided. State parameters that are normally encoded as ordinary binary values are blinded and their order masked using randomized permutation tables. While a traditional DES implementation would **encode the input message** M as a 64-bit value, an exemplary embodiment of **the invention blinds M to produce a two-part value (M1, M2)** such that M1 XOR M2 corresponds to the "normal" message. ('783 Patent, Col. 2:25-33.)

FN10. Claim 1 of the '783 Patent provides:
A method for performing a cryptographic operation on a message, comprising:

(a) generating initial **unpredictable information;**

(b) using said initial unpredictable information, transforming an initial secret quantity into a plurality of

randomized quantities having a predetermined logical relationship thereamong; and

(c) performing a first step of said operation involving said randomized quantities in a hardware device to reduce the amount of useful information about said operation available from external monitoring of said hardware device.

Claim 2 of the '783 Patent provides:

The method of claim 1 wherein **said initial unpredictable information** includes a plurality of random values obtained from a **random number generator.**

FN11. Cryptographic operations are used for a variety of processes such as data encryption and authentication. In a typical symmetric cryptographic process, a **secret key** is known to two or more participants, who use it to secure their communications. In systems using asymmetric (or public key) cryptography, one party typically performs operations using a secret key (e.g., the so-called private key), while the other performs complementary operations using only non-secret parameters (e.g., the so-called public key). In both symmetric and asymmetric cryptosystems, secret parameters must be kept confidential, since an attacker who compromises a key can decrypt communications, forge signatures, perform unauthorized transactions, impersonate users, or cause other problems. ('783 Patent, Col. 1:17-30.)

N.D.Cal.,2007.
Cryptography Research, Inc. v. Visa Intern. Service Ass'n