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

Dec. 21, 2007.

Darren E. Donnelly, David Douglas Schumann, J. David Hadden, Laurie Charington, Lynn H. Pasahow, Fenwick & West LLP, Mountain View, CA, for Plaintiff.

SIXTH CLAIM CONSTRUCTION ORDER

JAMES WARE, **District Judge.**

I. INTRODUCTION

On October 16, 2007, the Court issued an Order requiring the parties to meet and confer and to submit a Supplemental Joint Claim Construction Chart addressing the remaining claims in dispute of the patents-in-suit. In compliance with the Court's Order, on October 29, 2007, the parties submitted a Joint Chart and a Joint Memorandum of Law. This Order addresses the claim language listed by the parties as remaining in dispute.

The legal standards for claim construction which were previously articulated by the Court apply to this Order.

II. DISCUSSION

A. *The '658 Patent*

1. Claim 39 of the '658 Patent

Claim 39 provides: FN1

A method for implementing a private key operation for an asymmetric cryptographic system with resistance to leakage attacks against said cryptographic system, comprising the steps of:

(a) encoding a portion of a private key as at least two **component parts,** such that an arithmetic function of said parts yields said portion;

(b) modifying said component parts to produce updated component parts, but where said arithmetic function of said updated parts still yields said private key portion;

(c) obtaining a message for use in an asymmetric private key cryptographic operation;

(d) separately applying **said component parts** to said message to produce an intermediate result;

(e) deriving a final result from said intermediate result such that said final result is a valid result of applying said private key to said message; and

(f) repeating steps (b) through (e) a plurality of times.

The parties' sole dispute in this claim is the construction of the phrase "component parts." The dispute is whether the phrase should be construed to mean "updated component parts."

Claim 39 discloses a method which is a loop, with steps (b) through (e) repeated a plurality of times. The disputed phrase appears in step (d) which discloses that "said component parts" are "applied" to the message to produce "an intermediate result." The antecedent to the "component parts applied in step (d) is a portion of a private key encoded as at least two component parts in step (a) and modified in step (b). The plain language of the method discloses that "component parts" as used in step (a) means: components of a private key as originally encoded. Similarly, the plain language of the claim discloses that "component parts" as used in step (d) means: modified component parts which have been updated in accordance with the method.

In the specification, the inventors discuss various embodiments of protocols for dividing a private key into component parts and for updating the component parts. For example, with respect to the EIGamal protocol, the inventors state:

To make the EIGamal public-key decrypton process leak-resistant, the secret exponent (p-1-a) is stored in two halves a sub.1 and a sub.2 * * * The variables a. sub. 1 and a. sub. 2 are normally chosen initially as random integers between 0 and .phi.(p). Alternatively, it is possible to generate a first, then choose a.sub.1 and a.sub.2, as by selecting a.sub.1 relatively prime to .phi.(p) and computing a.sub.2=(a. sup.-1 mod .phi. (p))(a. sub. 1. sup.-1 mod .phi. (p)) mod .phi. (p).

FIG. 4 illustrates an exemplary leak-resistant ElGamal decryption process. At step 405, the decryption device receives an encrypted message pair (.gamma., .delta.). At step 410, the device selects a random r.sub.1 where 1.ltoreq.r.sub.1 <.phi.(p) and gcd(r.sub.1, .phi.(p))=1. At step 415, the device **updates** a.sub.1 by computing a. sub. 1.rarw.a. sub. 1 r. sub. 1 mod . phi. (p), **over-writing the old value** of a. sub. 1 with the new value.

('658 Patent, Col. 18:34-45.)

In this embodiment, after the initial iteration, the value of a component part is deleted in the updating process and the computation is performed with the updated component part.

Accordingly, the Court construes the phrase "**component parts**" as used in the ' 658 Patent to mean: **the initial or the updated component part encoded from a portion of a private key.**

2. Claim 47 of the '658 Patent

Claim 47 provides:

A method for performing cryptographic transactions in a **cryptographic token** while protecting a **stored cryptographic key** against compromise due to leakage attacks, including the steps of:

(a) **retrieving said stored key** from a memory;

(b) cryptographically processing said key, to derive an updated key, by executing a cryptographic update function that:

(i) prevents partial information about said stored key from revealing useful information about said updated key, and

(ii) also prevents partial information about said updated key from revealing useful information about said stored key;

(c) replacing **said stored key** in said memory with said updated key;

(d) performing a cryptographic operation using said updated key; and

(e) repeating steps (a) through (d) a plurality of times.

a. "a cryptographic token"

The Preamble to Claim 47 states a claim to "A method for performing cryptographic transactions in a **cryptographic token** ..." The parties dispute the construction of the phrase "cryptographic token."

In the patent documents, the inventors define the phrase:

It is currently extremely difficult, however, to make hardware key management systems that provide good security, particularly in low-cost unshielded cryptographic devices for use in applications where attackers will have physical control over the device. For example, **cryptographic tokens** (such as smartcards used in electronic cash and copy protection schemes) must protect their keys even in potentially hostile environments. (A **token** is a device that contains or manipulates cryptographic keys that need to be protected from attackers. Forms in which tokens may be manufactured include, without limitation, smartcards, specialized encryption and key management devices, secure telephones, secure picture phones, secure web servers, consumer electronics devices using cryptography, secure microprocessors, and other tamper-resistant cryptographic systems.)

('658 Patent, Col. 1:33-48.)

When an inventor act as his own lexicographer and use the specification to define a phrase used in a patent claim, the claim should be construed consistently with that definition. 3M Innovative Properties Co. v.

Avery Dennison Corp., 350 F.3d 1365, 1371 (Fed.Cir.2003). In this case, the inventors do not define "cryptographic tokens" in terms of their size. The only limitations stated by the inventors pertain to the functions of "cryptographic tokens," namely, containing or manipulating cryptographic keys.

Accordingly, the Court construes the phrase "**cryptographic token**" as used in the '658 Patent FN2 to mean: **a device that contains or manipulates a cryptographic key for purposes of its protection. Forms in which tokens may be manufactured include, without limitation, smartcards, specialized encryption and key management devices, secure telephones, secure picture phones, secure web servers, consumer electronic devices using cryptography, secure microprocessors, and other tamper-resistant cryptographic systems.**

b. "retrieving said stored key from a memory"

Claim 47 discloses a method for performing cryptographic transactions in a cryptographic token while protecting a stored cryptographic key. The first step in the method is "retrieving said stored key from a memory." The parties dispute the construction of the language used in this step. Specifically, the parties dispute whether the "stored key" should be defined in a manner which distinguishes it from a modified key such as the "updated key" disclosed in step (b). In addition, there is a dispute between the parties with respect to whether the "retrieving" step should be limited to being performed in an asymmetric system only.

The phrase "said stored key" refers to the antecedent "stored cryptographic key" disclosed the preamble to Claim 47. The method specifies a loop: the stored cryptograpic key is "retrieved" in step (a); "updated" in step (b); "replaced" in memory in step (c); "used" in a cryptographic operation in step (d); and upon initiation of a subsequent transaction, the "updated key" is "retrieved" from memory in step (e). In the method steps (a) through (d) are repeated a plurality of times. It is apparent from the plain language of the claim that the "cryptographic key" retrieved in step (a) is an unmodified key when the method is first practiced and is an "updated key" each time the method is executed.

An additional dispute between the parties is whether Claim 47 is limited to an asymmetric process. Neither the language of Claim 47, the specification, or the prosecution history FN3 limit the operation of the method to an asymmetric process. Moreover, because dependent Claim 49 limits step (d) to a "symmetric" cryptographic operation, claim differentiation leads the Court to presumes that step (d) in independent Claim 47 includes both symmetric and asymmetric operations. *See* Liebel-Flarsheim Co. v. Medrad, Inc., 358 F.3d 898, 910 (Fed.Cir.2004).

Accordingly, the Court construes the phrase "**retrieving said stored key**" as used in the '658 Patent to mean: **retrieving from memory a stored key, which initially is the original key, and thereafter, is a cryptographically updated key.**

B. *The '518 Patent*

1. Claim 2 of the '518 Patent

Claim 2 provides:

A method for performing **a balanced cryptographic operation** on input data, comprising:

(a) representing said input data using a **constant Hamming weight** representation; and

(b) using a secret key, manipulating said input data to produce output data by performing a **balanced cryptographic operation** thereon;

thereby cryptographically processing said input data in a manner resistant to detection of said secret key by external monitoring of a hardware device performing said cryptographic operation.

a. "a balanced cryptographic operation"

The parties dispute the construction of the phrase "balanced cryptographic operation." In the specification, the inventors describe a way in which attackers can extract secret information by monitoring variations in the electric current draw or electromagnetic radiation emanating during cryptographic operations. The inventors disclose that the purpose of the invention is to reduce the amount of secret information which is "leaked" by, among other things, methods which hold "invariant" the signals emanated during cryptographic operations:

The present invention reduces the amount of information about secret parameters leaked from cryptosystems. Sufficient leakage rate reduction can make a system secure by reducing the leakage rate to a low enough level that attacks are not feasible (for example, if the secrets will not be compromised within the device's operational lifetime).

The invention is described using embodiments including specialized data representations, methods of computation, and pre-or inter-computation state maintenance procedures. In these embodiments, sources of information leaked from a system, such as signals correlated to bit values, Hamming weights of the data, and state transitions during computational operations are held invariant with respect to the parameters of the computation.

('518 Patent, Col. 4:14-27.)

In the specification, the inventors describe a number of embodiments of the invention in which a cryptographic operation is performed in such a way that the externally monitorable signals do not vary with the parameters of the computation. For example, in one embodiment, the bit values in the operation are replaced with constant Hamming weights:

In the following exemplary embodiment of the invention, traditional representations are replaced with analogous constant Hamming weight representations. In the exemplary constant Hamming weight representation, each traditional binary digit requires at least one pair of lower level entities to be represented. a simple constant Hamming weight representation maps "one" onto the two-digit binary number 10, and "zero" onto 01.

('518 Patent, Col. 5:4-11.)

The inventors describe data with different values but with the same Hamming weight as "balanced" in that the computation would yield identical or very similar external signals:

Measurable external characteristics of such an operation are mostly or completely independent of the order of the bits within the input registers. For example, the processes of computing '0101 AND 0011' and '1100

AND 0110' are **balanced, i.e.,** they should have identical or very similar external characteristics."

('518 Patent, Col. 5:45-46.)

The specification discloses other embodiments which use alternative methods to reduce externally detectable signal variations. In one embodiment, variations in signals are reduced by keeping constant the number of transitions that take place in the course of a transaction so that the number of transitions is independent of the data parameters. ('518 Patent, Col. 5:32-64.) In other embodiments, the inventors describe how constant signals can be generated using leakless logic gates. ('518 Patent, Col 6:23-58.)

Accordingly, the Court construes the phrase **"a balanced cryptographic operation**" used in the '518 Patent to mean: **a cryptographic operation in which data is represented, computed or processed during the operation in a manner so that any variations in signals which might emanate during the operation cannot be feasibly correlated to the data which is being processed or the sequence of instructions being executed.**

b. "representing said input data using a constant Hamming weight representation"

In addition, the parties dispute the construction of the step "representing said input data using a constant Hamming weight representation." Since the specification does not contain a definition of "Hamming weight," the Court considers an art specific dictionary as instructive of the term's ordinary meaning. A technical dictionary defines "Hamming code" as an error correcting code for security of data that is represented by binary digits, which is named for R.W. Hamming of Bell Labs. *See* MICROSOFT COMPUTER DICTIONARY, 244 (5th ed.2002). Binary code is "weighted" by how many bits are "1's" or "0's". *Id.,* 565.

In addition, the inventors cite as a prior art reference to the '518 Patent, U.S. Patent 4,569,052 which contains the following definition:

Hamming weight is the number of ones in a binary word. For example, the Hamming weight of .0.1.0.111.0.1 is 5, since it possesses 5 ones.

('052 Patent, Col. 3:36-39.)

Finally, in the specification, the inventors disclose a process of replacing input data, which has variations in Hamming weight with data having a "constant Hamming weight:"

The present invention transforms the basic representation of data. A constant Hamming weight data representation replaces conventional bit representations commonly employed in the background art.

('518 Patent, Col. 2:57-60.)

Accordingly, the Court construes the phrase **"representing said input data using a constant Hamming weight representation**" as used in the '518 Patent to mean **transforming the input data so that different portions of the input data which have different Hamming weights have the same Hamming weights.**

2. Claim 11 of the '518 Patent

Claim 11 provides:

A balanced cryptographic processing device comprising:

(a) an input interface for receiving a first and a second input variable to be used as inputs to a computation, each input variable represented by at least a first bit and a second bit, where said representation has a constant Hamming weight;

(b) **a first computational unit** for performing a bitwise logical operation on said first bit of said first input variable and said first bit of said second input variable;

(c) **a second computational unit** for performing said bitwise logical operation on said first bit of said first input variable and said second bit of said second input variable;

(d) **a third computational unit** for performing said bitwise logical operation on said second bit of said first input variable and said first bit of said second input variable; and

(e) **a fourth computational unit** for performing said bitwise logical operation on said second bit of said first input variable and said second bit of said second input variable; thereby cryptographically processing said input variables in a manner resistant to detection by external monitoring of a hardware device performing said operations.

Claim 11 claims the invention of an apparatus. The parties dispute the construction of the language of Claim 11 with respect to whether the four "computation units" should be construed to require as a limitation that they operate simultaneously FN4 with each other.

Claim 11 describes limitations on the four "computation units" in functional language. Rather than describe the "computational units" by describing their physical structures, the Claim describes how they must function. Each unit must be configured so as to be capable of performing a bitwise logical operation FN5 on at least a first bit and a second bit of each of the representations of the two input variables.

The first computation unit must be configured to perform its operation on the first bit of the first input variable and the first bit of the second input variable.

The second computation unit must be configured to perform its operation on the first bit of the first input variable and the second bit of the second input variable.

The third computation unit must be configured to perform its operation on the second bit of the first input variable and the first bit of the second input variable.

The fourth computation unit must be configured to perform its operation on the second bit of the first input variable and the second bit of the second input variable.

The claim language does not disclose a limitation that the operations must be performed simultaneously.

In the specification, the inventors discuss embodiments which minimize leakage of data by "circuit matching"-by matching wire lengths-components to achieve simultaneity in the form of "equalized gate switching times." However, the invention does not claim simultaneous operation as a limitation:

When constructing a leakless (leak-minimizing) circuit, the effectiveness of the leak minimization process depends in some degree on low-level details of the circuit layout and design. Although it is not necessary, further leak reduction might be achievable with appropriate adjustments to a circuit. A first often-relevant consideration relates to the layout and routing of wires between components. Asymmetries in wire routing between leakless logic gates can introduce differences in capacitance, resistance, inductance, signal timing, etc., ultimately introducing differences in externally-measurable characteristics such as electromagnetic radiation and/or power consumption. A circuit designer can choose to lay out components gates, wires, etc. so that input and output lines are of equal lengths and have equivalent electrical characteristics. It is also possible, but not necessary, to apply logic design principles of the background art to equalize the gate switching times. Also, since small manufacturing differences can potentially introduce differences between otherwise equivalent operational units, identical NMOS transistors, pMOS transistors, etc. are desirable (as are balanced wire lengths, routing, capacitive loads, etc.). While assuring exact balancing is likely to be impossible, sufficient matching of components can prevent exploitable differences in externally-measurable characteristics. While not essential, logic design principles of the prior art should be applied to equalize gate switching time.

('518 Patent, Col. 15:36-59.)

The Court notes that in Claim 31, the inventors disclose a device comprising "a plurality of additional logic subunits of composition similar to said main logic units which operate **simultaneously** with said main logic units to balance the power consumption of the computation performed by said main logic units." ('518 Patent, Col. 22:13-17.) The Court presumes that the express requirement of "simultaneous operations" of units in one claim of a patent, means that simultaneous operations are not required in another claim in the same patent which describes the operations of similar units, but where the claim does not expressly require simultaneous operations. *See* Forest Laboratories, Inc. v. Abbott Laboratories, 239 F.3d 1305, 1310 (Fed.Cir.2001).

Accordingly, the Court declines to construe Claim 11 to require simultaneous operations of the "computation units." There is no other dispute with respect to the language of Claim 11.

3. Claim 31 of the '518 Patent

Claim 31 provides:

A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to the discovery of a secret by external monitoring, comprising:

(a) an input interface for receiving a quantity to be cryptographically processed and for converting said quantity into an expanded balanced representation; and

(b) a processing circuit operatively connected to said input interface and including:

(i) a plurality of main logic subunits configured to in compute the result of said cryptographic processing operation; and

(ii) a plurality of additional logic subunits of composition similar to said main logic units which operate simultaneously with said main logic units **to balance the power consumption** of the computation performed by said main logic units; and

(c) an output interface operatively connected to said processing circuit for outputting said result of said cryptographic processing operation.

Based on the considerations discussed in Section II(A)(1) above, the Court construes the phrase "**to balance the power consumption**" as used in Claim 31 of the '518 Patent to mean: **to offset variations in power consumption.**

C. ***The '699 Patent***

Claim 1 of the '699 Patent provides:

A cryptographic token configured to perform cryptographic operations using a secret key in a secure manner, comprising:

(a) an interface configured to receive power from a source external to said token;

(b) a memory containing said secret key;

(c) a processor:

(i) configured to receive said power delivered via said interface;

(ii) configured to perform said processing using said secret key from said memory;

(d) said token having a power consumption characteristic:

(i) that is externally measurable; and

(ii) that varies over time in a manner measurably correlated with said cryptographic operations; and

(e) a source of unpredictable information configured for use in said cryptographic operations to make determination of said secret key **infeasible** from external measurements of said power consumption characteristic.

The parties dispute the construction of the word "infeasible." In the specification, the inventors discuss some of the features which make determination of the secret key infeasible:

In a typical leak-proof design, with each new cryptographic operation i, the attacker is assumed to be able to choose any function F.sub.i and determine the L.sub.MAX-bit result of computing F.sub.i on the device's secrets, inputs, intermediates, and outputs over the course of the operation. The attacker is even allowed to choose a new function F.sub.i with each new operation. The system may be considered leakproof with a security factor n and leak rate L . sub.MAX if, after observing a large number of operations, an attacker cannot forge signatures, decrypt data, or perform other sensitive operations without performing an exhaustive search to find an n-bit key or performing a comparable O(2.sup.n) operation. In addition to choosing L.sub.MAX, designers also choose n, and should select a value large enough to make exhaustive search **infeasible.** In the sections that follow, various embodiments of the invention, as applied to improve the security of common cryptographic operations and protocols, will be described in more detail.

('699 Patent, Col. 5:39.) It appears from the specification that the inventors used "infeasible" with its ordinary and customary meaning, namely "not easily done; impractical." *See* WEBSTER'S NEW TWENTIETH CENTURY DICTIONARY, 937 (2d ed.1983).

Accordingly, the Court construes the word **"infeasible"** as used in the '699 Patent to mean: **impractical.**

D. *The '884 Patent*

Claim 4 of the '884 Patent provides:

An integrated circuit device configured to perform a cryptographic transformation on an input to produce an output using a secret key contained in said integrated circuit, comprising:

(a) a data interface configured to communicate at least one of said input and said output to said cryptographic transformation; and

(b) a plurality of interconnected operation modules for use in performing said cryptographic transformation on said input to produce said output, configured such that:

i) each said operation module is connected to at least one data input; and

(ii) each said operation module is connected to a power source; and

(iii) each said operation module is configured to consume a nonconstant amount of power from said power source during computation of said cryptographic transformation; and

(c) said device being characterized in that key-dependent variations in said power consumption of each said operation module are **compensated by** one or more modules of said circuit configured to

(i) draw additional power upon decreases in said key-dependent power consumption, and

(ii) draw less power upon increases in said key-dependent power consumption,

thereby reducing key-dependent variations in said integrated circuit device's total power consumption and inhibiting determination of said key by monitoring power consumption of said integrated circuit.

The parties dispute the construction of the phrase "compensated by" as it is used in Claim 4. The phrase which appears in the claim is not used by the inventors elsewhere in the specification. Reading the language of Claim 4, it is plain that the phrase "compensated by" is not being used in any specialized or novel way. An ordinary and customary meaning of "compensated by" is "to supply an equivalent." *See* WEBSTER'S NEW TWENTIETH CENTURY DICTIONARY, 370 (2d ed.1983). It is apparent from the plain language of Claim 4 that variations in power consumption of key-dependent operation modules are "compensated by" other modules, i.e., as the key-dependent module decreases its power consumption, the other module "compensates" by drawing additional power. Likewise, as the key-dependent module increases its power consumption, the other module compensates by drawing less power.

Accordingly, the Court construes the phrase "**compensated by**" as used in the ' 884 Patent to mean: **offset by.**

III. CONCLUSION

Having construed the claims as indicated, the Court orders the parties to appear for a Case Management Conference on **January 15, 2008 at 10 A.M.** to coincide with a hearing on various motions previous noticed for that day. FN6 Pursuant to the Civil Local Rules of Court, the parties shall meet and confer in good faith to develop a Joint Case Management Statement addressing further proceedings in the case in light of this Order and a schedule for those proceedings. The parties shall file their Joint Statement by **January 9, 2008.**

FN1. Unless otherwise indicated, all bold typeface is added by the Court for emphasis.

FN2. This construction also applies to the phrase "cryptographic token" in Claim 1 of the '699 Patent, which is a divisional patent based on the same specification as the '658 Patent.

FN3. At the Court's request, the parties submitted relevant portions of the prosecution history. Although office actions discuss whether certain claims in the application were drawn to asymmetric processes, the inventors did not limit the claim eventually allowed as Claim 47 to an asymmetric process.

FN4. Since the disputed language is in an apparatus claim, the Court rejects proposed constructions proffered by both parties insofar as they ask the Court to construe the language of the claim as "steps"-a construction appropriate to a method claim.

FN5. Although one skilled in the art reading the patent specification at the time of the invention would understand that each computation unit includes logic gates, the components of a circuit are not disclosed. Figure 6 illustrates an embodiment of a circuit. However, Claim 11 is not limited to that embodiment.

FN6. The hearing is at 9 A.M. and the conference is at 10 A.M.

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

Produced by Sans Paper, LLC.