Hash Algorithm Case
Intellectual Property High Court
Case No. H19 (gyo-ke) 10239（February 29, 2008）

FACTS

Plaintiff, who is a juridical person in the United States of America, filed a patent application for inventions to be described hereinafter (“present inventions”) entitled “Methods for producing a shortened representation of a collection of bits,” received a decision of rejection, so the plaintiff filed an appeal against the decision, received an appeal decision dismissing the appeal, and thus, sought a rescission of the appeal decision.

The scope of claims upon the first amendment (February 9, 2004) consists of, as mentioned, claims 1 to 4, and the subject matters are as follows (hereinafter, referred to as "present invention 1" to "present invention 4" in the order as described and collectively referred to as the "present inventions").

1. An apparatus of producing a shortened representation of a collection of bits, comprising:
summing a key having at least "n" bits with an input collection of "n" bits to produce a sum;
squaring the sum to produce a squared sum;
performing a modular "p" operation on the squared sum, where "p" is at least as large as a first prime number greater than 2^n to produce a modular "p" result;
performing a modular 2^l operation on the modular "p" result to produce a modular 2^l result where, "l" is less than "n"; and
outputting the modular 2^l result.

2. An apparatus of producing a shortened representation of a collection of bits, comprising:
summing a first key having at least "n" bits with an input collection of "n" bits to produce a first sum;
squaring the first sum to produce a first squared sum;
summing the first squared sum with a second key having at least "n" bits to

produce a second sum;
performing a modular "p" operation on the second sum, where "p" is at least as large as a first prime number greater than 2^n to produce a modular "p" result;
performing a modular 2^l operation on the modular "p" result to produce a modular 2^l result where, "l" is less than "n"; and
outputting the modular 2^l result.

3. An apparatus of producing a shortened representation of a collection of bits, comprising:
summing a key having at least "n" bits with an input collection of "n" bits to produce a sum;
squaring the sum to produce a squared sum;
repeating the previous three steps at least once to produce a plurality of squared sums, where a different key is used each time the steps are repeated;
summing the plurality of squared sums to produce a summation;
performing a modular "p" operation on the summation, where "p" is at least as large as a first prime number greater than 2^n to produce a modular "p" result;
performing a modular 2^l operation on the modular "p" result to produce a modular 2^l result where, "l" is less than "n"; and
outputting the modular 2^l result.

4. The apparatus according to claim 1, 2 or 3, wherein the apparatus is a communication apparatus using the produced shortened representation for a message authentication.

ISSUE

Whether the present inventions which relate to a computational technique (algorithm) for high-speed computer processing by means of a hash method, which is a method for converting a long data string into a short data string for data operation, fall within the purview of an “invention” as set forth in Article 2 Paragraph 1 of the Patent Act and by extension the main clause of Article 29 Paragraph 1 of the same Act.

HOLDING

Incidentally, a solution or mathematical computational procedure (algorithm) itself to the above described mathematical problem is a pure academic principle and does not utilize any law of nature, and therefore, it is apparent that this cannot said to be an invention as set forth in Article 2 Paragraph 1 of the Act. Furthermore, because processing a mathematical formula using an existing arithmetic device is nothing more or less than a realization of a solution or a mathematical computational procedure for the above described mathematical problem, this does not add any technical idea utilizing the laws of nature. Therefore, an apparatus that processes a mathematical formula such as the present inventions cannot be an invention unless some creation based on the technical idea in the apparatus itself is found (if this were assumed to be an invention, then every mathematical formula could be an invention.).

In this regard, the plaintiff has acknowledged himself that the present inventions do not add any novel feature to the processing device itself, and even in view of the description of the scope of claims, the "apparatus of producing a shortened representation of a collection of bits" is merely "producing a modular result" for each of the above and "outputting" the modular result, which defines nothing about the processing device according to the use purpose, so, in a manner of speaking, it is nothing more than defining an "apparatus" computing the above described mathematical algorithm.

In that case, because the present inventions do not add any novel creation to the existing processing device, and the substance thereof is nothing more or less than a mathematical algorithm itself, it cannot be said that this falls under the purview of an "invention" as set forth in Article 2 Paragraph 1 of the Act.