UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,

Petitioner,

CERTIFIED COPY

v.

WARD PARTICIPATIONS B.V.,

Patent Owner.

Case IPR2022-00113 (US Patent No. 10,992,480)

Case PGR2022-00007 (US Patent No. 10,992,480)

Case IPR2022-00114 (US Patent No. 11,063,766)

VIDEOCONFERENCE DEPOSITION OF

DR. BART PRENEEL

November 4, 2022

Page 1 - 70 8:13 a.m. EST - 10:39 a.m. EST

REPORTED BY:
Tamara L. Houston
CA CSR No. 7244, RPR, CCRR No. 140
Job Number 22-117175
Ref. 39843-0109IP1; 39843-0109PS1; 39843-0110IP1

REMOTE VIDEOCONFERENCE DEPOSITION OF DR. BART PRENEEL taken on behalf of the Petitioner, commencing from 8:13 a.m. EST to 10:39 a.m. EST, Friday, November 4, 2022, before Tamara L. Houston, CSR No. 7244, CCRR, RPR.

APPEARANCE OF COUNSEL:

On behalf of the Petitioner:

FISH & RICHARDSON P.C.
BY: USMAN A. KHAN, PH.D., ESQ.
JEREMY MONALDO, ESQ.
1000 Maine Avenue SW
Suite 1000
Washington, DC 20024
(202) 626-6383
khan@fr.com
monaldo@fr.com

On behalf of the Patent Owner and Witness:

RAMEY LLP
BY: JACOB B. HENRY, ESQ.
5020 Montrose Boulevard
Suite 800
Houston, Texas 77006
(832) 454-1456
jhenry@rameyfirm.com

ALSO PRESENT: Scott Ward, Proprietor

INDEX TO EXAMINATION

WITNESS: DR. BART PRENEEL

QUESTIONS INSTRUCTED NOT TO ANSWER

Page	Line

None

INDEX TO EXHIBITS

DR. BART PRENEEL

SAMSUNG ELECTRONICS CO., LTD. vs. WARD PARTICIPATIONS B.V.

November 4, 2022

Tamara L. Houston, CSR No. 7244, CRR No. 140, RPR

EXHIBIT	DESCRIPTION	PAGE

None.

--o0o--

Friday, November 4, 2022, 8:13 a.m. EST

--o0o--

Whereupon, DR. BART PRENEEL, having been called as a witness was duly sworn to tell the truth, the whole truth, and nothing but the truth testified as follows:

EXAMINATION BY MR. KHAN:

Q. Good afternoon, Dr. Preneel. I hope you're well.

A. Good morning.

Q. I wanted to first check with you and see if -- if you are in -- do you have -- have you taken any medication today or anything that would prevent you from speaking about your declaration?

A. No, I have not.

Q. Okay. Thank you.

So like the deposition earlier this week, I'll start off with some general questions before getting into more specifics. I'll provide you breaks periodically unless you specifically request them. Should you or Ms. Houston or anyone else here feel that we need to take a break, I'll request that you just give me a heads-up so I can wrap up the line of questioning.

Does that work for you?

A. That's fine.
Q. And during the breaks, you understand that you're not allowed to discuss the substance of your testimony today with counsel of Ward?
A. I understand it.
Q. And would you agree to let me know if anyone at any point communicates with you in any manner during the course of the cross-examination regarding your testimony today?
A. Yes, I will do that.
Q. Okay. Do you understand that you are being deposed today for statements made in your declarations submitted in support of Ward's two patent owner responses in -- with respect to the '480 patent?
A. I do.
Q. And that the proceeding numbers are PGR2022-0007, and IPR2022-00113?
A. Yes, they are.
Q. For purposes of our deposition today, when I refer to "your declaration," I will be referring to the declaration you submitted in the PGR proceedings, which is PGR2022-0007 --
A. Okay.
Q. -- unless I specifically mention the other declaration.

Does that sound okay to you?

A. That's fine.

Q. Great.

Do you agree that your testimony on both of those declarations substantively overlaps?

A. Yes, I do.

Q. So if I ask you a question regarding your PGR declaration, it would also apply to your IPR declaration; is that correct?

A. That is correct.

Q. Thank you.

Do you understand that your testimony today is sworn testimony taken under oath?

A. I understand that, yes.

Q. And do you understand that the oath you've taken in this deposition today is as solemn as the oath you would take if testifying at trial?

A. I understand that, yes.

Q. Do you understand that the deposition testimony today can be used at a trial or subsequent briefs in these proceedings?

A. Yes, I understand that.

Q. Did you review your declarations in the '480 patent in preparation for this deposition today?

A. Can you please clarify the question?

Q. Sure. Did you -- did you review your declarations in the '480 patent in preparation for the deposition today?

A. Yes, I did.

Q. And I know I asked you this in the beginning of the call, but is there any reason why you would not be able to speak to your declarations with full clarity today?

A. No, there is not.

Q. In preparation for the deposition today, did you confer with Ward's counsel?

A. We had a preparatory meeting on Monday, so before the first deposition.

Q. Okay. And between the first deposition, which was held on Tuesday for the '766 proceedings, and today, have you been in communication with Ward's counsel?

A. No, I have not been in communication with Ward's counsel in that period.

Q. Okay. So is it -- is it correct to say that you -- is it -- is my understanding correct that you were not provided any feedback on your testimony with respect to the '766 deposition conducted earlier this week from Ward's counsel?

A. No, I was not.

Q. Okay. Thank you.

Now, turning to the '480 declaration that you submitted, did you write that declaration yourself?

A. Yes, I did.

Q. How long did it take you to write the declaration?

A. I mean, I don't have recollection of the details because this work was done almost a year ago, but, of course, I spent a considerable amount of time studying the patents and studying all of the documents provided to me. So I think it was definitely an effort of I think 10 to 15 working days, at least.

Q. I see.

A. And then I wrote -- of course, then the writing of the text is -- just takes a few days --

Q. Did you draft all the parts yourself?

A. Of course, at the beginning, I think there is some understanding of the applicable legal standards, and yes, I was provided this. And of course, I went to this and I made sure that I fully understood this.

Q. Okay. With respect to your '480 declarations, are there any statements or remarks that you would like to change?

A. No, there are not any.

Q. Now, to avoid -- well, as you know, the '766 and '480 have references that overlap and also share the

same specification, so to avoid repeating many of the questions and answers from our last session, I'll just ask a few questions to confirm the applicability of some of the questions that I asked earlier in the '766 deposition and how they may relate to today.

So in our last deposition on Tuesday addressing the '766 declaration, do you agree that I asked you questions on your background, such as your experience?

A. Yes, I do.

Q. Are your answers to those questions the same today with respect to the '480 declaration as they were on Tuesday?

A. Yes, I confirm that those answers also apply to the '480 declaration.

Q. We also discussed your views on the '766 patent, its disclosure such as the figures in -- such as Figures 3 and Figures 4 on Tuesday.

Do you agree that your views on the disclosure in the '766 patent also apply to the '480 patent?

A. There are, of course, differences between the two patents, but where the patents are identical, of course, my views are identical.

Q. Okay. And what are those differences between the two patents?

A. Well, it's not so easy to answer that very briefly, but I think there are differences. In particular, when we look at Claims 17 and 18, where there is a substantial difference in the sense that here it is explained very clearly that a private key can also be stored in a memory -- not necessarily in BIOS or a secure memory -- and then this would be protected under the keys securely stored, but this is a substantial difference between the two patents.

And I think a second difference related to protection of authentication software --

(Court reporter requested clarification.)

THE WITNESS: Second difference relates to the protection of the authentication software.

And let me confirm that I have my note correctly. In '480, the software is not necessarily encrypted. It can be encrypted, but it is not necessarily encrypted.

BY MR. KHAN:

Q. So when you say in '480 it is not necessarily encrypted, are you saying that the -- the discussion of the description of the encryption in '480 is different than the one in the '766?

A. Yes, because in '480, it may be encrypted but does not need to be encrypted.

Q. I'm sorry. Could you repeat that, please? What was that?

A. In '480, it may be encrypted, but it does not need to be encrypted.

Q. And that's because the '480 describes it differently than the '766?

A. Yes, it does.

Q. So -- but with respect to our discussion, would you agree that Figures 3 and Figures 4 of the '766 patent are the same as Figures 3 and Figure 4 of the '480 patent?

A. Yes, they are.

Q. And to the extent that I had asked you questions about Figures 3 and Figures 4 with respect to the '766 patent, would you agree that your answers to those questions also are applicable to the '480 patent?

A. It depends on a specific question, obviously. I mean, a figure only makes abstractions and shows only a high level view. If you go into the details, as I mentioned in my previous answer, there may be subtle differences.

Q. Okay. We'd also discussed your views on the Ellison reference. Are your views on the Ellison reference the same as they were on Tuesday?

A. Yes, they are.

Q. Okay. If I could ask you to open up your declaration, please, and turning to paragraph 26.

A. Yes.

Q. So like in your '766 declaration, you noted that you used the BRI standard.

Did you use the same BRI standard to interpret the '480 claims?

A. Yes, I did.

Q. Okay.

A. Could you confirm which paragraph this was? Because I opened the '007 PGR document and paragraph 26 --

Q. Yes. Paragraph 26 reads, "Patent claims in a PGR are given their broadest reasonable interpretation ('BRI')."

Do you see that?

A. So we need the number of the document just to be sure.

Q. So the -- it should be in link that I sent to you --

A. Yes.

Q. All right. In that link, you should have seen a file -- let's see. It should -- the filing should be -- it should have your declaration.

A. Yes. The "Preneel '480 PGR Declaration."

Q. That's right.
A. Yes.
Q. Yeah, so if you could open that file.
A. Yes, I did that.
Q. Great. And then paragraph 26 of that file.
A. 26 reads for me, "I have been part-time advisor at Phillips Research."
Q. Okay. One second, please. Okay. I'm sorry. It should be paragraph 37.
A. Okay. Thank you.
Q. I'm sorry.
So paragraph 37 states, "Patent claims in a PGR are given their broadest reasonable interpretation ('BRI')."
Is that correct?
A. That's correct.
Q. So is it correct that you used the BRI standard to interpret the '480 claims?
A. Yes, I did.
Q. The last sentence on that same paragraph reads, "The patent's entire disclosure, including the specification and prosecution history, should be considered to understand the BRI."
Is that correct?
A. That is correct.

Q. So just to clarify, the last three words -- the last phrase that ends that sentence, the "should be considered to understand the BRI," did you mean to say that the patent's entire disclosure, including the specification and prosecution history, should be interpreted under the BRI?

A. I can guess, I think, in the formulation for me.

Q. Okay. All right. So it's correct to say that in reviewing the '480 patent and the description of the prosecution history and the claims, you -- you used the broadest reasonable interpretation standard?

A. That is correct.

Q. Okay. Thank you.

Now, in the following paragraphs after that, for example, in paragraphs 40 to 42 -- actually, 40 to 45, like in the '766 declaration, you discuss the legal standards that you use; is that correct?

A. That is correct.

Q. Now, we had discussed on Tuesday your understanding of the BRI standards like the IPR and PGR obviousness and anticipation. Is that still the same? Are your views and your understanding of these concepts -- these legal concepts still the same as they were on Tuesday for the '766?

A. My views and understanding are still the same.
Q. Thank you.
I just want to get a better sense here. In paragraph 41, you mention anticipation. And I wanted to ask you if a combination of two references can anticipate a claim.
A. I think it says so in the 42, "A claim can be obvious when its elements are disclosed in two or more references from the prior art, and there was a reason for a person of ordinary skill to combine those references to obtain the elements as claimed."
Q. So I'll just repeat the question.
A. Okay.
Q. Can a combination of two references anticipate a claim?
A. So if -- I think I can only repeat the same answer that, in fact, if two elements are disclosed in two references from the prior art and there was a reason for a POSITA to combine those references, then it can be prior art.
Q. Okay. So if I can repeat the answer, my understanding of your answer, when I asked you if combination of two references can anticipate a claim, you indicated that your answer is in paragraph 42, which states that, "A claim can be obvious when its elements

are disclosed in two or more references from the prior art."

Is that correct?

A. And there was a reason for a POSITA to combine those references.

Q. Okay. Thank you.

So in paragraph 42, you mentioned that, "A claim can be obvious," right, "when its elements are disclosed in two or more references from the prior art."

Can a claim be obvious in a combination of five or six references?

A. I think it can be, but the approach that we do is -- I think it's the work step by step. And of course, again, all the disclaimers have to apply. Also for more than two, of course, so that the POSITA should have a reason to obtain these elements of the claim. It's not the existence of the references that is sufficient.

Q. When you say "all of the disclaimers have to apply," I'm not sure what you mean. Could you clarify, please?

A. Well, because in your question you did not add the phrase "and there was a reason for a person of ordinary skill to combine those references."

Q. I see.

In addition to what you said there, you quote the language, "and there was a reason for a person of ordinary skill in the art to combine those references." When you look at two references, what are some of the factors you consider when determining whether prior art renders a claim obvious?

A. I think there has to be a natural way of combining these things, so it's the case when you combine things, I should not have to come up with a new invention or new innovative step to actually achieve the claim that would be obvious. So it should be actually rather easy to take the two elements and to combine them based on, I would say, standard expertise available to a POSITA. I think that's an important element. The combination should not by itself require an inventive step.

Q. So when you are considering whether two references can be combined, is it correct that your conclusion would depend on whether there is some type of inventive step involved in the combination of those two references? Is that correct?

A. That is correct.

And I think a second element -- may I add, which is the last sentence in paragraph 42, of course, if you would in the combination render one of the

references inoperable for its intended purpose, then of course, you also don't have obviousness.

Q. Did you review the petition, the '480 petitions, the PGR and IPR petitions?

A. Yes, I did.

Q. And is it your understanding that both of those petitions include obviousness grounds?

A. Yes. I understand that.

Q. And so did you also use the obviousness standard to analyze the '480 patent?

A. Yes, I did.

Q. Okay. So in considering the -- like the claims and the written description and the figures, you considered the obviousness standard and then also applied the same standard for the prior art; is that correct?

A. Yes, that's correct.

Q. Thank you.

In the PGRs, there's a 112 ground, 35 USC 112 ground.

Are you familiar with what the 35 USC 112 ground is?

A. I'm afraid that I don't know the articles of that all. I'm a technical expert, and I don't know the details of a number. I guess I could review the

legislation and what I should use on these techniques, but if you give me a number, I'm afraid I can't reproduce the exact condition behind that.

Q. Yes. So in the PGR, there was a ground indicating that the '480 claims did not have written description.

Do you recall that?

A. I think I do. Yes.

Q. Now, are you aware that there is a statute requiring a patent to provide a full written description for its claims' subject matter?

A. Yes, I understand that. That's the purpose of a patent is to, of course, give the description and then give the claims, and indeed, the claims should be substantiated by the description.

Q. And you understand that if it does not provide the written description, then it can be found invalid; is that correct?

A. Yes, I understand that.

Q. Thank you.

MR. KHAN: Can we take a two-minute break?

THE WITNESS: That's fine.

MR. KHAN: Great. Thank you.

(Recess: 8:41 a.m. to 8:47 a.m.)

BY MR. KHAN:

Q. So, Dr. Preneel, in the chat I shared another file, if you don't mind downloading that.

A. I have downloaded the file.

Q. Great. Thank you.

So that is -- my apologies for the slight confusion there. I think moving forward we'll use this file. This is -- this is your PGR declaration. Your previous file, so far we've discussed, had the same contents, but I believe it was your earlier declaration. So it had the same paragraphs just numbered differently. It was from your earlier declaration. So --

A. Okay.

Q. Yeah, so I just -- you know, if you can open that up, I'll confirm with you just that, for example, the paragraphs we've been discussing -- this is Exhibit 2012 -- the paragraphs we discussed were the paragraphs related to the BRI standards, which you can see in paragraph 26.

A. Yes, that's correct.

Q. Confirmed.

And we also discussed the anticipation and obviousness standard that you can see here in paragraphs 30 to 34.

Is that correct?

A. Yes, these are the same paragraphs.

Q. Great. Thank you. And my apologies there again.

So turning to Exhibit 2012, in paragraph 46. In paragraph 46, you state here that, "It is important to point out that in cryptography private keys are either bit strings, that is, finite sequences consisting of binary zeroes and ones or algebraic objects."

Is that correct?

A. That is correct.

Q. Is it your position that that private keys can only be bit strings or algebraic objects?

A. Well, they can always be represented as such.

Q. So just -- just the two of them? Just the two, the bit strings or algebraic objects; is that correct?

A. Well, you could choose -- if you invent the private key or crypto system in which a private key is words in a language, but you would still always be able to represent those as bit stings, because you can represent the characters at bit strings.

(Court reporter requested clarification.)

THE WITNESS: Yes. So you can -- you can -- you could invent a cryptographic system in which the keys are words in a natural language, but you could

always represent those words character by character as bit strings.

BY MR. KHAN:

Q. So you agree that a private key can only be a bit string or an algebraic object?

A. I don't think that's what I said in my previous answer. But I think in this comment in cryptography, if you take the standard used algorithms, which are in -- cryptographic standards are in textbooks, they will have indeed keys consisting of binary strings or algebraic objects which can be represented by binary strings.

Q. So I suppose I'm trying to understand that. When you said that the private keys -- so is it correct in paragraph 46, you say, "Cryptography private keys are either bit strings, that is, finite sequences consisting of binary zeroes and ones or algebraic objects."

So my question --

A. I can represent that as finite number of bit strings.

Q. Yes. Well, my question is very -- because you used the word "either," I'm trying to understand that -- do you mean, then, that all cryptography private keys can just be either bit strings or algebraic objects?

A. I think, indeed, that's what's the case in all

crypto systems that are being used and that are being described in textbooks.

Q. Is that the case for the disclosure in the '480 patent as well?

A. Yes, it is.

Q. So any bit string in the '480 patent can -- sorry. On any private key in the '480 patent, in your opinion, could only be a bit string or algebraic object; is that correct?

A. Represented as a bit string, yes.

Q. So what are algebraic objects?

A. An algebraic object is an object described by mathematics. This is typically --

(Court reporter requested clarification.)

THE WITNESS: -- an algebraic object such as a group, a ring, or a field which has elements and operations on those elements.

BY MR. KHAN:

Q. And what is a bit string?

A. A bit string is a finite sequence consisting of binary zeroes and ones.

Q. Can a single bit be a bit string?

A. Yes, it is. It is finite and it consists of zeroes and ones.

Q. Does it have to have any structure to it, or

is it just a sequence of finite numbers? Zeroes and ones?

A. Well, this is exactly why I have the definition I give. So it's a finite sequence of zeroes and ones or it's an algebraic object because that has some structure into it.

Q. I was asking you about -- I'm sorry. I was asking you about a bit string. In your -- what is a bit string?

A. A bit string is a finite sequence of zeroes and ones.

Q. Does it have structure?

A. Not necessarily but, of course, it can have structure.

Q. Like what?

A. For some reason, you could decide to always have two zeroes and two ones and two zeroes and two ones, and you have a bit string with structure in itself. Or you would have a bit string in which every four consecutive bits amount to an integer between --

(Court reporter requested clarification.)

THE WITNESS: Or you can have a bit string in which every consecutive sequence of four bits represents an integer between zero and nine.

BY MR. KHAN:

Q. So in this example you just gave, when -- I guess by structure, you mean pattern, like you could have the -- the sequence of bits could correlate to a particular patent pattern -- is that --

A. For example, yes.

Q. Okay. So a bit string could be a sequence of -- a finite sequence of zeroes and ones in -- according to some pattern or, in some cases, no pattern; is that correct?

A. That's correct.

Q. And I guess, are there any other structural or pattern requirements there; or is it just as long as you have a finite sequence of binary zeroes and ones, you have a bit string?

A. If you have -- if I have a sequence of binary zeroes and ones, you have a bit string. Requirements on the pattern would come from the cryptographic algorithm for which it is intended, where it was a key.

Q. I see.

Can a computer have more than one bit string?

A. Yes.

Q. Are -- are all authentication tables bit strings?

A. Yes, they can be represented as bit strings.

Q. My question was, are all authentication tables

bit strings?

A. All authentication tables can be represented as bit strings.

Q. You say "can be." What do you mean by "can be"?

A. Because you could also represent it in other ways, potentially.

Q. So if -- if authentication tables can be represented in other ways, then all authentication tables are not bit strings; is that correct?

A. But if you write it in a computer, they will end up being bit strings because that's how computers represent objects. So if I have an authentication table of any form or shape and I want to load it into a computer, it will be there as a bit string. I will be able to point to a bit string in the computer corresponding to this authentication table.

Q. So you mentioned the authentication table may have a form and a shape.

What type of form and shape do authentication tables have?

A. That depends on the specific algorithm selected. A natural way would be just a list of bit strings where it has an index, an address running from, say, 0 to 1 million, and for each entry you have a bit

string of, say, like, 64 bits. But you could also choose to have a table that again consists of a million entries where each entry consists of six digits between 0 and 9.

Q. So --

A. They would represent those in the computer, they would be again represented as bit strings, but with a specific structure as we discussed before.

Q. Does an authentication table have rows and columns?

A. It can be organized as a linear table with rows, but it can also be organized as a matrix with rows and columns.

Q. Does an authentication table have index to specify a row and a column?

A. If the table consists of rows and columns, it will have an index for the rows and an index for the columns.

Q. What type of rows and columns does an authentication table typically have?

A. I think that's a question which that's hard to answer. It depends on the application. But typically, like, I can give an example of an authentication table, but there could be other applications or other context where we have different tables. But one could have a

table with, say, a thousand rows and a thousand columns, and then there would be in this table a million values, or bit strings, if you want to be in my definition.

(Court reporter requested clarification.)

BY MR. KHAN:

Q. Why are authentication tables used?

A. They can be used to authenticate a data item or can be used to authenticate a person or a device.

Q. And what's the advantage of using an authentication table versus a bit string?

A. Well, authentication table in the computer would be represented as a set of bit strings. So in the end, in that respect, there is not much difference. It's just a different way of doing things. You can authenticate data with a cryptographic algorithm. It uses as key a bit string, or you could decide to authenticate a data item using authentication table. It's one way of -- another way -- there are different ways of achieving the same goal.

Q. So if I may repeat your answer, you mentioned that there's different ways to authenticate, and one way is to use an authentication table, and another way is using a bit string, and there are different ways of performing the authentication; is that correct?

A. Well, they will be used in combination with a

different authentication algorithm. And if you use a table, you will have a bit more data to store, but you may have fewer computations. If you use a short bit string, you need obviously to store fewer data, but you may have to do more computations.

Q. So the advantage of using a table, authentication table, is that you will need to perform fewer computations, and the disadvantage is that you would have to store a bit more data; is that --

A. That's correct. Yes.

Q. And so is it fair to say that when you're interested in performing a faster computation, you may want to use a authentication table?

A. That is correct, yes.

Q. And you mentioned you might have to store a bit more data; is that correct?

A. That's correct.

Q. What's that -- what's the additional data that you typically store?

A. Well, you have to store authentication table which consists of multiple bit strings.

(Court reporter requested clarification.)

BY MR. KHAN:

Q. And is it multiple bit strings because you have different rows and columns?

A. In each row and column element, you have to store, indeed, a table element, and that's a bit string.

Q. So authentication table will have different elements, and each element is a bit string; is that correct?

A. That's correct, yes. Or it can be represented as a bit string.

Q. And each element may have -- each element has a row and column assigned to it that's part of the authentication table; is that correct?

A. I would formulate it the other way around. I would say to each row and column, you assign an element.

Q. Okay. And in order to do that, you would need to also have information about the row number and the column number; is that correct?

A. Can you clarify? In order to do what?

Q. So in order to store different elements or different bit strings in an authentication table --

A. Yes.

Q. -- is it correct that you would then need a mechanism to identify where in the table that particular element or bit string is?

A. Yes. You have an index for the rows and an index for the columns, and these are, again, bit strings.

Q. Is there a type of -- sorry. Are there bit strings that are not authentication tables?

A. I think it's very hard to answer this question because I could always, in principle, construct an authentication table that corresponds to a certain bit string if this bit string has sufficient length.

Q. I'll repeat my question because I'm not sure you've answered the question.

My question was, are there bit strings that are not authentication tables?

A. I think the answer is no because even a bit string -- a single bit string is a table with one row and one column and a corresponding authentication table with one entry.

Q. Okay. So is -- I'm sorry. Can you still hear me? My computer froze up a little bit. So just give me a second.

A. I can hear you.

Q. Okay. Is a software identification number an authentication table?

A. No, it's not an authentication table. An authentication table is just --

(Court reporter requested clarification.)

THE WITNESS: Sorry. No, it is not an authentication table. That was my answer. Apologies.

BY MR. KHAN:

Q. Going back to your declaration, paragraph 46. At the end of 46, you state -- so you state that, "The use of the terms authentication data and bit strings in '480 can be deduced from the following examples."

Is that a correct reading of that sentence in paragraph 46?

A. That is correct.

Q. And is it correct that in the following examples that you mention, you point to three examples: In column 4, lines 33 to 39; column 7, lines 45 to 48; and column 10, lines 23 to 33 of the '480 patent?

A. That is correct.

Q. Is it correct that not a single one of these quoted passages recites the words "authentication data"?

A. It is correct. Yes.

Q. To your knowledge, "authentication data" is recited in other parts of the '480 patent; is that correct?

A. That is correct.

Q. In paragraph 47 and I guess subparagraph g, it's on page 19 of Exhibit 2012.

Do you see that?

A. Yes.

Q. And this -- here you're quoting column 9,

lines 35 to 56 of the '480 patent; is that correct?

A. That is correct.

Q. Now, in this section, g, you have italicized one sentence and bolded the following sentence. That the sentence -- sorry.

You've italicized two sentences and bolded the sentence that follows the italicized two sentences; is that correct?

A. That is correct.

Q. Was there a reason why you italicized one and bolded the others? I'm just trying to understand, you know, what the difference was.

A. I think they're just key points of this paragraph I wanted to draw the attention to.

Q. Now, in these key points, you mention a Ring 0 processing environment; is that correct?

A. That is correct.

Q. What is a Ring 0 processing environment?

A. That's a processing environment of a processor with the highest privilege.

Q. When you say "highest privilege," can you clarify what that means?

A. It means that this environment can access information which higher rings -- Rings 1, 2, and 3 and so on -- cannot access. So it's used to control the

processor and to organize the processor.

Q. So is it correct to say that Ring 0 has the least level of access privileges?

A. I would prefer to rephrase that and say as the highest level of access privileges in the sense that it can do more, but of course, fewer entities have access to this. So the user applications do not have access typically to Ring 0.

Q. Now, you used the word "typically."

Does that mean that in some cases it can be accessed by user-operated software applications?

A. I think it's real applications can request the kernel running in Ring 0 to do certain things, but they cannot see what is happening there. Why do I say "typically"? Because people have conceived operating systems where there is no separation between user and kernels, so very simplified systems. And there have been cases where there were flaws in the kernel software giving the users this kind of access. But if a computer is probably -- properly configured and operated, user applications will not have access to the Ring 0.

Q. So is it fair to say, then, that in some systems, user applications can have access? Those would be the simpler systems. And in other systems, the user applications are restricted from access at Ring 0; is

that correct?

A. I would rephrase this because, maybe to clarify, when I speak of those simpler systems, those are typically not systems with users. Those are systems operating a washing machine or systems operating sensor notes. But if we have user applications, which means we have browsers and word processing tools, then they will not have access to Ring 0.

Q. So your answer -- last answer mentioned the word "typically" again. Just to clarify, I'm not asking for the typical situations. I'm asking about what's possible, right? And so when I ask you about user applications, you know, I'm asking, is it possible that some user applications have access to Ring 0 and in other systems the user applications do not have access to Ring 0? Is that correct?

A. If I give my answer for Windows machines, macOS, and Linux machines, they have no access.

(Court reporter requested clarification.)

THE WITNESS: Windows machines, macOS, so the -- like the Apple systems, and the Linux systems -- user applications will not have access to Ring 0.

BY MR. KHAN:

Q. So if you limit to Window machines or -- I'm sorry, micro -- what was it? Micro?

A. MacOS, operating system by Apple. And I think also --

Q. I see. I see. Okay.

A. I should also add the mobile devices, Android and iOS.

Q. And so when you say it has the highest level of access privilege, Ring 0 -- is that correct?

A. That's correct.

Q. Is it correct to say that it also is the most restricted level of -- of the rings in the sense that whatever processing goes on in Ring 0 can be restricted to the highest degree compared to the other Ring levels?

A. Yes, fewer processors have access to this.

Q. Turning to paragraph 54 of your declaration. Please let me know when you're there.

A. Yes, I'm there.

Q. Is it correct that paragraph 54 states, "The '480 patent does not provide the authentication software" -- sorry -- sorry, scratch that.

It says, "The '480 patent does not provide that the authentication software would have (undefined) access to its own private key by requesting such access from any other software component."

Is that correct?

A. That is correct, yes.

Q. Can you clarify what you mean by "undefined" here?

A. I think "undefined" means here in a not previously specified way. And it could also -- so, for example, it could be read access or write access, or what is meant is any form of access.

Q. So is it -- is my understanding correct if I interpret that as saying that the '480 patent does not provide that the authentication software would have predetermined access?

A. I would say any form of access.

Q. Any form of access.

So it would have any form of access, or it would not have any form of access?

A. Does not provide that authentication software would have any form of access to its own private key by requesting such access from any other software component.

Q. So what you're saying -- in paragraph 54, you're saying, the '480 patent does not provide that the authentication software would have any form of access to its own private key by requesting such access from any other software component; is that correct?

A. Yes.

Q. When would the authentication software request

access from another software component? Access to its own private key?

A. One can imagine that this private key is under control of another process and has to have access to this. Imagine a very simple example where you would work with a smart card, insert it in the computer. Then authentication software would have to request access to this smart card.

Q. In that example of the smart card, is the private key the smart card's private key, or is the private key the authentication software's private key?

A. It could be the key stored in the smart card, and I guess given that we use the term "software component," we should speak of virtual smart card. So it could be the private key of the authentication software but stored in some other piece of software, such as a virtual smart card.

Q. So in that example that you're saying, the authentication software's private key is stored somewhere else, not with the authentication software, and in that case, it would be requesting access to whichever other storage or memory component that might be storing that private key; is that correct?

A. That is correct.

MR. KHAN: We've been going a little bit over

an hour, so if you'd like to take a break here, you know, it might be a good time to take a break. Now would you like maybe a ten-minute break?

THE WITNESS: Okay.

MR. KHAN: Great. Thank you.

(Recess: 9:27 a.m. to 9:37 a.m.)

MR. KHAN: I think at the beginning we didn't note all of the attendees today. Do you want to make a note of that now?

(Discussion off the record.)

MR. KHAN: Okay. Yeah. I think it will be great to have it on the record.

So on the Petitioner's side, we have myself, Usman Khan, and my colleague, Jeremy Monaldo.

And, Jacob, if you'd like to talk about the patent owner's --

MR. HENRY: Sure. On the patent owner's side, we have myself, Jacob Henry, we have Dr. Bart Preneel, and observing is patent owner, Scott Ward.

MR. KHAN: Thank you.

MR. HENRY: You're welcome.

BY MR. KHAN:

Q. Great. So I'll continue.

So before the break, we were at paragraph 54 and I was asking for some clarification regarding the

term "undefined."

I wanted to get a little bit more clarification on some of the discussions in the declaration. In paragraph 40 -- so in paragraph 46 and in a few other places, you use the term "can be," right? So, for example, in paragraph 46, the first sentence -- you talked about this earlier -- you'd mentioned, "The finite sequences consisting of binary zeroes and ones or algebraic objects (such as two prime numbers, finite field elements) that can be represented as a finite number of string bits [sic]."

Is that correct?

A. That's correct, yes.

Q. Okay. So you mentioned the word "can be" -- words "can be" in a few different places, and I wanted to understand that when you say "can be," do you mean it's possible? Or do you mean something else?

A. Well, in this case it means it's possible, but of course, as I mentioned before, if you represent it in a computer, then you will do it as a finite number of bit strings.

(Court reporter requested clarification.)

THE WITNESS: But if you do a calculation on paper, you could work with digits 0 to 9.

BY MR. KHAN:

Q. So when we say that -- as an example, when we say "X can be Y," is it correct that, consistent with your use of the word "can be," "X can be Y" would mean that X can, in some cases, be Y and, in other cases, does not have to be Y; is that correct?

A. I'm not sure this is the correct interpretation here. And in any case, we would have to do it for every occurrence. I'm happy to repeat the clarification I gave.

So I think here "can be" means it is technically possible to do this, and the additional clarification provided is that this is the way that it is done in computer systems.

Q. Okay. So maybe we can re- -- maybe we can visit some of the other iterations of the phrase "can be." In paragraph 55 -- please let me know when you're there.

A. Yes, I'm there.

Q. Paragraph 55 states, "Because the private key can be an integral part of the authentication software"; is that correct?

A. That is correct.

Q. So here, when you say "private key can be an integral part of the authentication software," are you

saying it's technically possible that the private key is an integral part of an authentication software?

A. Yes, it is.

Q. And paragraph 55, you have no citation to that statement you made; is that correct?

A. That is correct.

Q. So is it correct that the private key can also not be an integral part of the authentication software?

A. That is correct.

Q. So when you make the statement "the private key can be an integral part of the authentication software," is that -- kind of when you're interpreting the '480 patent in view of the obviousness standard, you're saying, "Yeah, it would be obvious that the private key can be an integral part of the authentication software"; is that correct?

A. That is correct, yes.

Q. Turning to paragraph 67. Please let me know when you're there.

A. Yes, I'm there.

Q. In paragraph 57 [sic], you state, "In the '480 patent, a private key can be authentication data."

Is that correct?

A. Yes.

Q. So consistent with your earlier statement,

here when you say "a private key can be authentication data," are you saying that it's technically possible for a private key to be authentication data? Is that correct?

A. That is correct.

Q. And consistent with the meaning of that term, it's also possible that the private key cannot be authentication data; is that correct?

A. That is correct.

Q. And so when you make the statement "a private key can be authentication data," it's again because a person of ordinary skill in the art would have found it obvious in view of the '480 patent; is that correct?

A. That is correct.

Q. In paragraph 94, please let me know when you're there.

A. Yes, I'm there.

Q. Paragraph 94, the last three words, the closed parentheses that says, "Insert references here."

Is that correct?

A. That is correct.

Q. Was that a typo?

A. I think that was intended to be corrected, but then due to time pressure, apparently this did not happen. But I'm sure that counsel, if that would be

allowed, can provide you with those references later on.

Q. So as the declaration was submitted, there's no citation to any references in paragraph 94; is that correct?

A. That is correct.

Q. Would you also agree that there is no citation in the entire Section B of your declaration which extends from paragraph 52 to 71?

A. I would have to clarify that.

Q. Please go ahead and take your time.

A. That is correct.

Q. Is it also correct that paragraphs 76 to 95 in Section D of your declaration include no citations?

A. That is correct, but I want to point out that they do refer to Ellison and Muir, the specific numbers in the figures in those patents.

Q. You mean like the reference numbers in Ellison and --

A. Yes.

Q. I see.

But there's no citations; is that correct?

A. No. That is correct.

Q. So is it fair to say that from paragraphs 52 to 71 and 76 to 95, you describe the references and make technical points without a single citation?

A. That is correct, yes. But these things -- but these statements are -- in having obtained as a consequence of careful study of the references, including the patents.

Q. What is an encryption key?

A. Can you refer to a specific clause in this document, or is there a figure in the patent you want me to refer to?

Q. No. Just generally, what's your understanding of what an encryption key is?

A. An encryption key is a key used in a cryptographic algorithm.

Q. How is it used?

A. Can be used to encrypt data but can also be sometimes used to decrypt data because the key for encryption and decryption can be the same. An encryption key can also be used to authenticate data or to verify authentication of data, and obviously an encryption key can also be used to encrypt or decrypt another key.

Q. So if an encryption key is not used to perform encryption, is it still an encryption key?

A. An encryption key can be used for multiple purposes, and sometimes the same key is used for multiple purposes and it will still be called an

"encryption key."

Q. So I'll repeat my question because I don't think it was fully answered.

My question was, if an encryption key does not perform encryption, can it still be called an encryption key?

A. My statement would here be that if you write a scientific paper, you would probably use a specific term for this and you would not do this. I have seen in patents sometimes that encryption key is used as a more general term for a cryptographic key. So a key used for any algorithm, also another algorithm for encryption and decryption.

Q. So in the context of the '480 patent, when you see an encryption key -- for example, encryption key 46 in Figure 3 --

A. Yes.

Q. -- is that a -- just a general cryptographic key, or is it performing encryption and decryption or both?

A. I think to answer that exactly, I would have to go through all of the uses in the description of the patent, but the first purpose is indeed encryption and decryption of data or a key. But it could be that you can actually authenticate data by encrypting it, and

then the operation done with an encryption key is an authentication.

(Court reporter requested clarification.)

THE WITNESS: To use an encryption key to -- sorry. I'm not sure I can rephrase it exactly the same.

But one could use an encryption key to authenticate data as well. An encryption key can be used to encrypt data as a form of authentication. Maybe that's a better way of expressing it.

BY MR. KHAN:

Q. So if a key performs authentication but does not perform encryption, are you saying that that key can still be called an encryption key?

A. I think that would be possible, yes. It would not be my preferred terminology, but I think it would be possible.

Q. So in your opinion, an encryption key -- I'm sorry. In your opinion, a key can be an encryption key even though it does not perform encryption?

A. Yes, that would be possible.

Q. And so if there is a authentication key that performs no encryption or decryption, it could be called an encryption key; is that correct?

A. I think that would be possible. Again, it would not be my preferred way of denoting it, but it

could be understood like this, yes.

Q. Why would it not be your preferred way?

A. Because it's easier to clearly indicate what the purpose of a key is, and it is in general better to use a key only for one purpose. But there are applications where these rules are not followed.

Q. Does the '480 patent follow those rules or does not follow those rules?

A. I would have to double-check this, but I don't think it follows those rules completely.

Q. And what makes you think that?

A. I think I would have to go to detailed references to point out where these keys are being used in which way.

Q. Okay. If you'd like to take the time to do that, we can -- we can do that.

A. You want me to find all of the occurrences, or would it be okay if I find just one of them?

Q. Yeah, I think one of them is fine.

A. So in Patent '480, column 5, lines 39 to 43, "The authentication software preferably has its own unique serial number, software ID and/or private encryption key."

Q. So does that -- and this is column 5, lines 39 to 40; is that correct?

A. That's correct.

Q. Does it tell you there whether it uses that private encryption key for encryption or other purposes?

A. Well, it leaves it open, but the software could use this key also for authentication.

Q. I see. And so this is because a person of ordinary skill in the art looking at this description would have found it obvious in view of what a private encryption key is; is that correct?

A. That's correct. Yes.

Q. So can an encryption key be a public encryption key, or can it also be a private encryption key?

A. An encryption key can be a public encryption key, but then we use a different form of cryptography called asymmetric encryption where we have a different key for encryption and decryption. And in that case, the encryption key can be public but the decryption key is always secret.

But if we have symmetric cryptography, then we use the same key for encryption or decryption, or at least a decryption key can be derived easily from the encryption key. And in that case, of course, it cannot be made public because that would defeat the purpose of having encryption.

Q. So if I understood you correctly, you're saying that when we use symmetric encryption, an encryption key cannot be a public encryption key. When we use asymmetric encryption, then we can have a public key and some other form of a public key; is that correct?

A. When we use asymmetric encryption, we have a public key for encryption and a private key for decryption.

Q. Right. Okay. And is the encryption key used to encrypt any kind of data?

A. An encryption key can be used to encrypt data or keys, yes.

Q. So -- I see.

So an encryption key can be used to encrypt a private key?

A. That's correct.

Q. So when we say an encrypted private key, that's a private key that has been encrypted; is that correct?

A. That is correct.

Q. And when we say a private encryption key, that is a key that is private that is used to perform encryption; is that correct?

A. I think we've been there before. So private

means you don't make it public. But as I explained, the term "encryption key" can also -- is also sometimes used for other cryptographic algorithms such as authentication algorithms.

(Court reporter requested clarification.)

BY MR. KHAN:

Q. The encrypted private key -- is an encrypted private key a -- essentially a private key that has had some form of encryption performed on it? Is that correct?

A. That is correct.

Q. But a private encryption key does not have to have had any encryption performed on it yet; is that correct?

A. The term "private encryption key," here private means that it should be protected, so it should remain confidential or private. So it has to be protected either by encrypting it or by storing it in a memory that is not accessible to unauthorized parties.

Q. Sorry. Private encryption key can be one that is stored in a protected location?

A. That is correct, yes.

Q. Do you agree that the term "private key" is recited in the '480 claims?

And we can just look at --

A. I have the -- yes, the term "private key" is used in this area. Yes, of course.

Q. Do you agree that the term "private key" is recited in the '480 patent in the paragraph beginning on column 13, line 31?

A. Yes, that is correct.

Q. And what does this paragraph say that the private key can be?

A. I will read the paragraph. "In a further embodiment, the authentication software may be provided with a system for signing a digital signature according to the present invention using at least a part of a software authentication number (software ID) or any other application identifying character string, hereinafter referred to as a private key."

So could you please repeat your question so I'm sure that I answer it correctly?

Q. My question was, how does this paragraph describe what a private key is?

A. This says that part of a software identification number or any character string that identifies an application can be used as a private key.

Q. Is a software ID number an encryption key?

A. A software ID number is a bit string and can be used as an encryption or authentication key. I think

here specifically it will be used for signing a digital signature, so it will be used for authentication. But as we discussed before, for such kind of key, sometimes the generic term "encryption key" is used.

Q. So I heard you say that the software ID can be an encryption key again. But I was asking you, to be more clear, does the '480 patent teach that the software ID number can be an encryption key?

A. What this paragraph teaches is that at least part of a software ID number, in this case it's an encryption key for assigning a digital signature.

Q. Can you tell me where in that paragraph it says "encryption key"?

A. It doesn't use this term, but as we discussed before, the term "encryption key" is used in the broader sense in these patents --

Q. Okay. So --

A. -- and the cryptographic key.

Q. So you're saying that even though this paragraph doesn't describe an encryption key, it would have been obvious that the private key is the encryption key; is that correct?

A. If people would refer to this key as an encryption key, I would understand what is meant by it, yes.

Q. I'm sorry. Can you repeat that, please?
A. If someone would refer to this private key as an encryption key, I would refer -- I would understand what is meant by it, yes.
Q. I guess I can ask you. I've wanted to ask if someone said it. I was asking if the '480 patent says it.
So do you know if the '480 patent says that the software ID number can be an encryption key?
A. In this paragraph, it doesn't say this.
Q. But --
A. But I think --
Q. Sorry. Go ahead.
A. But I think in the paragraph we discussed before, that the term "encryption key" was used in a broader sense.
Q. Which -- that was the paragraph describing the authentication software; is that correct?
A. That's correct, yes.
Q. And that was in column 5, lines 39 to 40; is that correct?
A. That's correct.
Q. So you're saying that someone looking at column 5, lines 39 to 40, and someone looking at column 13, lines 31 to, say, 56 or so would have

understood that a software ID can be a private -- can be an encryption key; is that correct?

A. That's correct, yes.

Q. And that's because it would have been obvious to a person of ordinary skill in the art reading those two passages; is that correct?

A. Yes.

Q. Okay. Even though it does not -- the '480 patent does not explicitly say so; is that correct?

A. That's correct.

Q. That same paragraph in column 13, lines 31 onwards, that starts off with the phrase "in a further embodiment"; is that correct?

A. Yes, that's right.

Q. What does embodiment mean to you?

A. It means a specific realization of the system described in the patent or matter described in the patent with some of the elements specified.

Q. So in this paragraph when they say "in a further embodiment," what's your understanding of what they mean by "further embodiment"?

A. It means that you specify more details.

Q. Is it the case that patents can have multiple embodiments, or do they have to have a single embodiment, like a single invention, single embodiment?

A. Patents can have multiple embodiments.

Q. Does -- is it your understanding that basically what we're seeing here in column 13, line 31 onwards, it's just another embodiment that is described by the '480 patent? Is that right?

A. That's correct. Yes.

Q. And that when you look at this embodiment and combine it with the other embodiments that are disclosed in the '480 patent, that it would have been then obvious that it discloses a private key in the manner that's claimed; is that correct?

A. That's correct.

Q. And is that how you also arrived at your statement in your declaration in paragraph 53?

A. Let me go back to that statement. Yes, indeed.

Q. Then going back to the column 13, line 31 onwards, that particular passage discloses that the second transaction party only stores the signed digital signature and that the private key is generated by a third party and sent to the second party for storage; is that correct?

A. That's correct.

Q. This passage does not describe a second party as providing the private key; is that correct?

A. I will have to read the full paragraph in detail before I can confirm that.

Q. I'm sorry. I should have given you time to read it first, so please take your time to read it.

A. Okay. Can you now please repeat your question?

Q. Yes. My question is that -- actually, I'll restart my line of questioning.

So do you agree that this passage discloses the second transaction party as only storing the signed digital signature and that the private key is generated by a third party and sent to the second party for storage?

A. That is correct. Yes.

Q. This passage does not describe the second party as providing the private key; is that correct?

A. That is correct.

Q. The private key is provided by the third party; is that correct?

A. That is correct.

Q. When the third party is providing the private key and the transaction is between the first transaction party and the second transaction party, would the third transaction party provide the private key to both the first transaction party and the second transaction

party?

A. No, it would not. What is described here can be summarized as outsourcing the verification of the digital signature to a TTP.

(Court reporter requested clarification.)

THE WITNESS: Outsource. Digital signature verification to a trusted third party.

BY MR. KHAN:

Q. Could you please explain why it wouldn't provide the private key to both the first transaction party and the second transaction party?

A. I think the model described here is different. So in order to reduce the cost and the efforts of the second party in the transaction -- that could be, say, the merchant who sells good -- rather than having the merchants buy and operate infrastructure to store keys and verify transactions, the merchant will only store the signature with the transaction and then ask the third party later in case of dispute to perform the verification. And because the second party does not do the verification, it does not need the keys.

Q. Okay. So it -- it just -- so the second transaction party here just stores the digital signature but never has any access to the private key; is that correct?

A. That is correct.
Q. Okay.
MR. KHAN: Can we take a ten-minute break, please?
(Recess: 10:18 a.m. to 10:26 a.m.)
BY MR. KHAN:
Q. So returning to the declaration, Section B on -- starting on page 22 of your declaration, that's entitled, "The Disclosure of the '480 Patent to One of Ordinary Skill in the Art"; is that correct?
A. That is correct.
Q. And in paragraph 52, you note that, "Each limitation is fully supported by the written description of the '480 patent and that one of ordinary skill in the art would readily recognize that the claim limitations are based on the disclosure of the '480 patent."
Is that correct?
A. That is correct.
Q. And they would readily recognize the claim limitations based on the disclosure of the '480 patent in view of the obviousness standard that you've applied consistently in reading the prior art and the '480 patent; is that correct?
A. That is correct.
Q. In paragraph 65, you refer to, "The '480

patent describes the claim features of Claim 2"; is that correct?

A. Yes, I do.

Q. Is there a discussion in your declaration as to Claims 4 and 5 of the '480 patent?

A. No, there was not, I think, but I believe the patent is clear in this respect.

(Court reporter requested clarification.)

THE WITNESS: Clear in this respect. Easy to understand in this respect.

MR. KHAN: Thank you. No further questions from me.

Jacob, would you like to redirect?

MR. HENRY: Yes, I just have a couple of questions, Dr. Preneel.

THE WITNESS: Okay.

EXAMINATION BY MR. HENRY:

Q. Earlier there was a discussion of bit strings and authentication tables. Do you remember that you were asked about those terms?

A. Yes, I do remember that.

Q. Okay. Did you mean to say that all bit strings correspond to authentication tables?

A. I think that's not really what I wanted to say. I think authentication table -- an authentication

table can be mapped to a bit string. Okay? And, of course, in a specific context where application tables are used, there is a one-to-one mapping between authentication tables and bit strings or every bit string corresponds to an authentication table and every authentication table corresponds to a bit string.

Q. But more generally in computing, bit strings are used and exist but do not correspond to authentication tables, correct?

A. That is correct. For example, if I have the key of an encryption algorithm, then that's a 158-bit, 192-bit, or 256-bit string that does not correspond to an authentication table.

Q. Earlier this morning you were asked about the difference between the '480 patent and the '766 patent. And the word "describes" was bandied about.

Do you remember that?

A. Yes, I do remember.

Q. The difference between the two patents lies in what they claim; is that not true?

A. That is correct.

MR. HENRY: Okay. I pass the witness.

MR. KHAN: Thank you. I have a few follow-up questions.

MR. HENRY: Did you say "no follow-up

questions"?

MR. KHAN: No. I said I have a few follow-up questions. Thank you.

FURTHER EXAMINATION BY MR. KHAN:

Q. So, Dr. Preneel, I just would like to get some clarification. We talked about bitstreams [sic] and authentication tables just now. And I think there's a little bit of confusion because of the words "can be," right? Maybe we can speak about it in the context of the '480 patent specifically.

In the '480 patent, are the authentication table -- are all the -- are the bit strings authentication tables?

A. Some bit strings are and some are not. One can implement the '480 patent where it's symmetric traditional cryptography as well and using -- for example, for encrypting a key or also for generating a digital signature, one can just use a bit string that does not correspond to an authentication table.

Q. Now, we had earlier talked about some advantages and disadvantages of using authentication tables and bitstreams. And you had mentioned that it's advantageous to use an authentication table perhaps when you need to perform fewer computations; is that correct?

A. That is correct.

Q. Is that also the case for the '480 patent?
A. That is correct, but that does not mean that one has to use everywhere authentication tables.
Q. So some places where '480 patent talks about a bit string, it could be authentication table, and other places it may not be authentication table; is that correct?
A. That is correct.
Q. And vice versa. In some places where it says "authentication table," it could be a bitstream or it could be something else?
A. Every authentication table will be represented in a computer system by a bit string.
Q. Did you say "bit string" --
A. I said that before.
Q. -- or a "bitstream"?
A. "String." I think we've been using -- maybe I misheard. But it's indeed not the word "stream." It's "string." We've been discussing "bit string" definition.
Q. And the authentication table in the '480 patent would also have rows and columns; is that correct?
A. It would have rows and columns, but one could have a case, as I -- we discussed before, there's only

one row and one column.

Q. And to identify the rows and columns, it -- typically it would use an index system to identify which row, which column; is that correct?

A. Yes. One would have a bit string indicating the row and a bit string indicating the column.

Q. So in an authentication table in the '480 patent, you'd have the bit string indicating the row and the column, a bit string which is the element within the table as well; is that correct?

A. That's correct. All the -- both the integers and the table values would be bit strings.

MR. KHAN: Great. No further questions.

MR. HENRY: I have no further questions.

COURT REPORTER: Counsel, may I get transcript requests on the record, please.

MR. KHAN: Yes, please. If we could get a rough draft today, that would be great.

COURT REPORTER: Of course.

MR. KHAN: Thank you.

COURT REPORTER: Mr. Henry, would you like a rough --

MR. HENRY: Yes. Yes, please.

COURT REPORTER: Would you like a rough as well?

MR. HENRY: If it's not too much trouble.

COURT REPORTER: Not at all.

MR. HENRY: Okay. That sounds great, then. Thank you.

(Whereupon the proceedings concluded at 10:39 a.m.)

ERRATA SHEET

NAME OF CASE: SAMSUNG ELECTRONICS CO., LTD. V. WARD PARTICIPATIONS B.V.
DATE OF DEPOSITION: NOVEMBER 4, 2022
NAME OF WITNESS: DR. BART PRENEEL

Reason Codes:
1: To clarify the record.
2: To conform to the facts.
3: To correct transcription error.

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

_____ _____
DR. BART PRENEEL DATED

DECLARATION UNDER PENALTY OF PERJURY

I, DR. BART PRENEEL, do hereby certify under penalty of perjury that I have read the foregoing transcript of my deposition taken on November 4, 2022; that I have made such corrections as appear noted on the Deposition Errata Page(s), attached hereto, signed by me; that my testimony as contained herein, as corrected, is true and correct.

This Declaration is executed this _____ day of _____, 20___, at _____, California.

_____

DR. BART PRENEEL

STATE OF CALIFORNIA)
) ss.
)

I, Tamara Houston, RPR, CCRR, CSR No. 7244, a Certified Shorthand Reporter in the State of California, duly empowered to administer oaths, do hereby certify:

That, prior to being examined, the witness named in the foregoing deposition was by me duly sworn to testify to the truth, the whole truth, and nothing but the truth;

That said deposition was taken down by me in shorthand at the time and place therein named, and thereafter reduced to typewriting by computer-aided transcription under my direction;

That the dismantling, unsealing, or unbinding of the original transcript will render the reporter's certification null and void.

I further certify that I am not interested in the event of the action.

In witness whereof, I have hereunto subscribed my name.

Dated: November 8, 2022

Tamara L. Houston

TAMARA L. HOUSTON
CSR 7244, RPR, CCRR 140