STEVE MILES: And so we started out with a little on the network. And it was a great deal of fun to think back and hear some of the origins of where some of the thinking was and to have a chance to discuss exactly where we are in the evolution of this-- either it's the internet of things, or according to Steve, it's things on the internet, whichever we decide it is. But we're going to move right into tags. And we have the director of the Auto-ID Labs at Fudan University in Shanghai, Professor Hao Min, who will start off the discussion.

HAO MIN: OK. And the whole RFID technology, I think, the first thing starting is from the RFID tags. So people are thinking about the tag, and what the performance of the costs of the RFID tag may just influence the adoption of this technology, because this is kind of the basis for this whole technology. So today I will talk about what's the user requirement for tags right now. And so this will promote us to research what the next generation we can do for the tag performance enhancement. And also, I'll introduce some new technologies being developed right now.

And there are many, already, some adoptions of this RFID technology. Some users are [? users ?] tags. So it's estimated that millions of tags be used right now. But there are still some problems.

People want a longer read range. Right now, a [INAUDIBLE] tag can reach the range of approximately 5 meters. But people are thinking about whether you need, like, 10 meters. If you reach 10 meters, more application will be wider.

The other thing that's really critical is the 100% read coverage. From the report from Walmart and the [INAUDIBLE], no one can reach 100% read right now, probably 99%, or someone even only gets, like, 90%. So what happens if 1% is still missing? So when we have any technologies, what we can improve that to get 100% read.

Also there's the issue is the people hope to get similar read performance in worldwide frequency, because in worldwide, the frequencies are very different, from [INAUDIBLE] to [INAUDIBLE] But different countries use different frequencies. But the tag is already there. The tag will move around the world, will be read in different frequencies.

Because of the RF properties of these tags, the read performance in different frequencies will be different. But people want that it should be almost a similar performance around the world. And so in that sense, the security and [INAUDIBLE].

Just the previous speakers from the web, they were all talking about securities. If there's no security, I think the RFID application will just get very limited. So just this [INAUDIBLE] say that the hack, EPC hack get attacked from-- I think it's from two days ago. So people pretend to be hack members, and they pull their posts on the hack. So all the hack members got all these junk mails.

So this is the issue, is when internet comes out, there's no security concerns. Internet comes from academics. So at first, DOD sponsor the program, and then grow and grow. Just no one is planning all the security issues on the internet. Right now the problems comes out. So right now we're talking about internet of things. We need to really think about the security issues.

So what we are doing right now? We are trying to improve the read range. Improve the read range is basically is to reduce the power consumption of the tag chip. If it consumes less power, than the read range will be longer.

So what we are doing is we try to improve the conversion efficiency for rectifier, because this is the IF signals coming from the reader and to the tag chip. And the tag chip will convert that into a DC, DC power, to a [INAUDIBLE] chip. So if you can improve the conversion efficiency, then it's the read range will get also improved.

And also, there are some special technologies being studied to reduce the power consumption. For example, as we called subthreshold digital circuits. If you have a background on digital circuits, we know why we need a power supply to power the digital circuitry, because the digital circuitry is a need to switch. But there's a threshold to switch the circuit on and off. So there is a threshold. But if the threshold is lower, then the voltage applied to that will be lower.

Right now there's a circuitry which we do not use the regular on and off mechanism. But we use a circuit called subthreshold. Even if you apply a voltage which is lower than the threshold, if still controls the circuit on off. Then this will reduce the power consumption.

And also there is a new circuit record called [INAUDIBLE] circuitry. Although this circuitry type is a long time ago, but recently we find out this probably can apply to the tag chip design. There's also some other conventional low-power circuit design technologies.

This is what we've done in recently. We recently published a paper here, published paper on the improved the rectifier efficiency by about 30% to 100%. That means double the efficiency. Normally, the efficiency is around, like, 20%, 30%. And we can improve it into 40% or 60%. Basically we use called a bootstrap to rectifier to get rid of the VT drop of the circuitry.

The second thing we are working on is there's a circuitry called adiabatic circuitry, which means the charge in the circuitry can be recycled. But previously, some people already published the papers. They used this adiabatic circuitry, but they convert it normally. Normally an electronic system is powered by a DC power. So they convert the DC power to a power clock, because adiabatic circuitry needs a power clock, and then convert-- and then to power the adiabatic circuitry.

But in RFID, because we already got the power supply from the radio way, radio signal. So the radio signal, it's already powered clock. It's already clock. So we can directly use that as the power clock. So then we can rid of the rectifier circuitry, so which eliminates the loss of the energy.

And also, it's because the adiabatic circuitry consumes less power than normal logic, then the whole power consumption of the tag is getting reduced a lot. By doing this, we estimated that probably we can get only 10% of the power consumption as normal circuitry. So this means what we can do-- we can increase the read range of the tag by a factor of 2 to 3.

Since I already talked about the subthreshold circuitry, this curve shows that the power consumption by a different power supply voltage. If we use the supply voltage of, say, less than the threshold voltage of a transistor, we may get four orders of magnitude of reduction of power consumption. But this circuitry has the limit of the working frequency is very low, probably only go to 1 meg.

We've got a simulation. If we let the circuitry only work at 1 meg, at 1 volt, a tag chip only consumes 10 nanoamp, which is only 1% of a normal power consumption of tag. By doing this, we may increase the read range by a factor of even 10.

And also, we are trying to figure out what really prevents your read from 100% of the tag. So why these missing tag? The tag is missing. A reason we find our way that if you put two tags next to each other, one is closer to the reader. Another one is behind that. And the one behind that will probably cannot be read. But if you remove the one closer to the read, the one there can be read. So look like the one closer to the reader masked the tags behind.

This is because the normal tag technology, they use a rectifier, because when the tag is closer to the reader, it gets more energy. So the energy goes into the tech needs to go somewhere. So it has a circuitry that convert it just to heat. So it consumes high power when the tag close to the reader. Because the tag consumes the power, then the magnetic wave will just stop there, will not go further into the tag after that.

So what we do, we are trying to have a new circuitry, which try when-- it detects whether the tag got enough power. If get enough power, it just tries to detune the tune circuitry so that it does not consume energy. It only absorbs energy it needed. All the other energy is just let go away. So this can have this tag behind that can get enough energy to get power. So this is we are doing. So what we are doing right now is so we can detect the power supply of the tag and then compare to a reference, and then try to tune the [? resonant ?] capacitor of the antenna. And it just makes it work.

Also, for the worldwide frequency of things, we also use this adaptive tag-- adaptive tuning waves. So it will detect the power. If get less power, it will try to tune the resonant cap to find a best point, which resonant at the frequency of the reader. So this make the performance get improved.

Also, security and [? authentications ?] get considered. So there will be a two-way [? authentication ?] is designed to both the reader-- you [? authenticate ?] the tags, and the reader tag get [? authentication ?] from the readers. But this is really challenging because the tag is so tiny chip, and it consumes less power. So it needs a low cost, low power. But it also needs adequate security between tag and readers.

We have tried a way which we integrate some [? authentication ?] into the gen 2 protocol to try to have the tag and the readers get authentication. We have some first simulations down. It kind of looks like work, but we still need a lot of work to do. OK, that's my presentation. Thank you.

[APPLAUSE]

STEVE MILES: And our next speaker is Sang-Gug Lee, who is an associate professor in the School of Engineering at the Auto-ID Labs at ICU Korea.

SANG-GUG LEE: Yeah.

In my talk, I would like to quickly go through the USN technology in Korea, and then we introduce what we are working on in Auto-ID Lab Korea. What I mean by "USN" is an Ubiquitous Sensor Network, which is known as a wireless sensing network. So the content would be some brief overview of what is going on inside Korea in this area, and then in relation to what's going on in Korea, what we are doing in Auto-ID Lab Korea.

Probably some of you are familiar with this A39. It's called the Information Technology A39 Strategy that Korean government came up with. And there are three areas where we are trying to promote services, and then three infrastructures, and then nine different areas of growth engine that the Korean government is working on.

And in this A39 strategy, you find that in the service area, the government is trying to provide the RFID-based services, and then also in the structure area by utilizing the Ubiquitous Sensor Network. We consider-- the Korean government considers-- Ubiquitous Sensor Network as one of the infrastructures that they would like to deploy in Korea, in South Korea. And then through that, hoping to be able to deploy these nine different area across engines.

And if we're being more specific with the time schedule, each of these nine areas, they have schedules, and then when they would like to-- what kind of technology for the commercialization. And if you look at the pink-colored icon there, this is the RFID and USN area, where the government is trying to commercialize a mobile RFID by year 2006, which is before the end of this year, and then hoping to be able to deploy the sensor tag or sensor node technology for the public application.

And the concept of a public ubiquitous sensor network is basically based on broadband convergence network, all these services, where the sensor network-based services would be available such that everywhere, everything with RFID tags. And we sense the sensing IDs and environmental information, and then real-time monitoring and the control through the network would be available. That's the idea here.

And the applications, I'm sure most of you are already familiar with. They are smart buildings, factory automation and monitoring, asset monitoring and management, structural health monitoring, and environmental monitoring. All this, we call this as a public ubiquitous sensor network technology. These are the targets the government is thrusting. And if you look at the technology tree, these are the infrastructures, studying the sensor, and then service available there.

While I was watching this morning, I was getting this philosophical question. We talk about all these technologies trying to make our life really easy and happy and all that. But I'm also, at the same time, finding out how all these technologies actually make our life miserable. You realize what I mean, right?

All these mobile phone technologies and internet. It seems like it's helping us in many different areas. But at the same time, we're finding ourselves running like crazy. It makes our life so busy. It doesn't really make our life happy. But I guess the race has started. It's just an unstoppable race that everybody has to run all at the same time.

But anyway, so these are what the government is trying to do, and this is their roadmap for actual milestones and roadmaps and how they would like to implement these technologies for the commercial applications. And in relation to that, what we try to do in Auto-ID Lab Korea is that-- these are what I have just talked about is basically of public ubiquitous sensor network technology that they try to deploy.

And in Auto-ID Lab Korea here, what we're trying to do is we try to make this public ubiquitous sensor network [INAUDIBLE] connected to the EPC network. So the theme of technology thrust in Auto-ID Lab Korea is EPC network base a sensor network technology. That's what we're trying to go after. And we have seven professors involved in this thrust coming from different backgrounds.

And our focus area is the hardware and communication technology for EPC-based next-generation ubiquitous sensor network, and some of the middleware technology for EPC sensor network, and then the privacy and security issues, as well as the business model development for the EPC sensor network applications.

And these are some of the research work that has been done as part of those thrust. And this is some hardware [INAUDIBLE] we've been working on the impulse radio development, which is being developed for the ranging and locationing. There's some typo there. We've been working on some pulse generator circuits, very low-power pulse generator circuits on that, and then also very low-power correlator circuits and stuff like that. So basically, we're working on transceiver designs, modems for some algorithms, and then for arranging and location purposes.

At the same time, we're also working on the reactive microradio technology, which means that the sensor responding to the signal. In other words, the sensor is under the sleep mode and responds only when it is being waked up by some wake-up signals, which is, I'm sure, a number of research institutes are working on at the moment.

Also, this is some of the work that we're working on on the sensor network [INAUDIBLE] architecture, where the circle area, I think, the whole [INAUDIBLE] represents the EPC network. And the circle part represents the area where in order for this EPC network being connected to the public ubiquitous sensor network system.

And we all saw some progress is being made in the secret and privacy area as well. And through all this activity-- in other words, [? RF-ran ?] chip sensor interfaces and networking and software, as well as a business application, privacy and security issue, we're hoping that the research that we're doing would be related to the future standardization that connects the public ubiquitous sensor network with the EPC network. That's it.

[APPLAUSE]

STEVE MILES: Our next speaker and member of the conference committee, Gisele Bennett from Georgia Tech.

GISELE BENNETT: All right, I am going to somewhat switch gears and go as quickly as I possibly can with the 10 minutes allocated with, I think, 30-some odd slides. And the whole point that I hope you walk away with is understanding the importance of requirements. We've talked about RFID, and we've talked about a number of applications. But understanding the requirements and what solution is going to meet your application is really critical.

And we had a project that I'm going to focus on, on a container project, and looking at sensors that have built-in-- tags that have built-in sensors to monitor the environment, to monitor the condition of an asset. And so this is one of my favorite slides because I think it goes back to World War II, if I'm not mistaken. And really, you're really trying to find something in all the things that we're talking about. RFID happens to be one mechanism.

And of course, the big motivator was the Walmart and the DOD. And one of my focus areas will be the DOD particular application. RFID's everywhere-- comes under different forms, different marketing, but everybody's pushing towards it. And really, as I indicated initially, asset tracking is really our focus. So if it's RFID, terrific. If it's some other mechanism, that's good too. Understanding the requirements is a really critical element to all of this.

As you can see-- and this is, I think, actually, I have to apologize, an old slide, because I'm sure the number of patents have actually increased beyond that in the RFID arena. I don't need to get into what automatic identification tracking is with this audience.

We've got a number of elements. We've talked about them in some of the other talks. We're going to talk about them-- they're going to come up in other discussions. But again, tracking something, storing information, and doing something with that data. All of these elements have come up in the talks. They're all critical elements, and they come in different shapes and forms.

Biometrics is another technology that should be looked at for security, authenticity. And that's something that might be integrated in-- not RFID, but integrated within the RFID systems, if you will, in data gathering.

Now, when I talk about requirements, this is one of my favorite slides, and I contribute this to Nick [? Toogis ?] from the DOD IAT office. And an understanding of requires is really critical.

So Walmart has been the pin-up CPG that gets referenced as the start of all of the RFID flurry, and DOD followed suit soon thereafter. But DOD can't really apply a lot of the commercial applications, because if they could, then their stores would move-- Walmart stores would move every so often.

Christmas would be a random event, maybe every five years, not once a year in December. The associates would be wearing different types of vests. And a stock-out means something completely different for the DOD than it does for Walmart. So understanding those requirements and the environment you have to work in kind of changes what technology you're going to use and how you're going to apply that technology.

The way we got into this, we were approached by the Navy to solve a problem of managing their high-value assets and, in particular, the engines. The problem is they were improperly stored and improperly tracked. So when they were able to find an engine that they were looking for, they were supposed to be in pretty good condition.

They'd find it floating in water. And thus, what was a perfectly good engine now had to be sent back to the depot. So you can imagine the cost, the readiness issues, all of the implications. And that's assuming you found the container that had that engine.

So with that, what we ended up doing is looking at an active RFID tag and looking at a tag that would monitor the container, which is the housing element for the asset that we were interested in-- not necessarily the container, but it was the asset-- and telling you where it was, what are the temperature conditions, what are the pressure conditions, was this container dropped, where has it been, and ultimately looking into, is it emitting a chemical when you get into Homeland Security issues.

And so we developed a tag, looked at common standards, integrated those standards onto a tag. And when you hear the various talks, you're going to hear about a number of issues of power, range for RFID, durability. And so what we looked at, and some of the interesting things that capitalize, actually, from the computer science world, is how do we network these tags? If we want to keep the power low, that's going to have an implication about how much distance and range we get. Now, these are active tags.

So with that, if we can implement kind of a hopping or-- and it's not really an ad hoc network, to say, but it looks like it-- where we can hop from tag to tag to tag to find the furthest tag away, without increasing power, without changing anything else, then we can form this network and get a map of where all our assets are. And so that's what we ended up doing to get around the power issue.

One of my last slides, I'll get into future technologies, and some of the things that we need to consider are power scavenging, ways to get power from other means. Especially when you're dealing with active systems where the power is self-contained, you've got to look at that because that's one of the greatest technology hurdles. And nothing to do with RFID, but it's a technology that has lots of research areas.

Contact memory buttons are something I pointed out early on. If you want to store asset information, maintenance history on an item, and be able to gather that without having to open up the container, find the paperwork, all of that can be integrated within your-- earlier there was mention about an architecture. Not only do you have a hardware architecture, but an information architecture that you're dealing with.

We had a pilot study, and everything you can think of that could go wrong went wrong. But finding power out in the field is a major issue. Having the ability to connect up to a computer without having to get lots of permissions was a major issue. In this particular case, luckily we didn't have any other RF interference conditions. But in a warehouse environment, what happened in an installation of an RFID system, it shut down the entire wireless network because they were incompatible.

So a lot of things that you've got to look at. It's not just a slap and chip and it's going to work. In our active case, if we had a forklift or something come in between the containers and the tags, and read rate stopped. What we're seeing on commercial data is that you'll have an item that goes from the back stock to the store, and then back again, and back and forth. Well, that's not happening. The accuracy that was discussed earlier is another critical issue.

What do you do with the data? Extremely important. And if you're not going to use the data, then why bother tagging your assets? And so that's another element that, I think, is now getting on the forefront.

And there are a lot of other, actually, side benefits that came about for this particular project. They were using brand new containers that were unpressurized, and so just the testing of the containers and making sure they're protecting the assets in itself was a side benefit that came out of that project.

So a lot of things to consider that we've talked about. Tag and label issue, these things are being discussed by various standards committees. Please follow those standards. The guidelines have been thought through very carefully. A lot of parameters-- we talked about how far, how fast, how much data, how much content, memory.

Security is another interesting component. And I never thought about somebody walking along the street with a reader and being able to decide which car they're going to break into based on the contents in the trunk until one of my students brought up that as an application or as a problem to solve.

And so there are a lot of things. Privacy, of course, is another big one. And other considerations, we'll get into in various talks on collisions. Lots of lessons learned, site surveys, power. The information system is very critical.

And where I think some of the future areas are-- and we've discussed these earlier-- include the various applications. The applications are endless-- nanotechnology, power sources, packaging, which will be a session tomorrow. How can we embed some of these things in the packaging that you're using to ship your assets?

And a term that we're using of performance based logistics, or logistical prognostics, taking algorithms that we use for predicting failures in equipment, and look at them for predicting failures in a logistics pipeline. These are all things to consider and take a look at. And lots of work, as Sanjay indicated, [INAUDIBLE]

[APPLAUSE]

STEVE MILES: And then Manfred Aigner, who's the group coordinator for the VLSI and security group at PROACT at the University of TU-Graz that has a joint research project with Phillips. And it's actually [? Ari Bachtel, ?] who's the head of EPC Global Europe, who suggested that we might want to consider some of the European experience with encryption in the smart card industry as it might relate to RFID.

MANFRED AIGNER: Thank you.

Thank you for the introduction. So it's a pleasure for me to present our results. We are involved in research for security tag, reader security on our RFID in, let's say, two or three years, involving from smart card implementations of crypto modules, [? NT ?] stuff.

And I'm happy to show you our results. I will talk a little bit of our group, what we are doing, and tell you the requirements we defined for our developments, and tell you the problems you face as a developer of crypto modules for tag application, and show you some of our results we achieved so far.

So we are a group of about 50 people doing research on IT security, from development of crypto algorithms-- Vincent Rijmen, the inventor of the Advanced Encryption Standard, is with us-- up to e-government applications. And I am the group leader of the group that is doing VLSI, so hardware implementations for crypto. We are doing implementations for smart cards, for embedded systems, accelerator cards for encrypted networks, [? NT ?] stuff. We are also doing a lot of system and chip design.

Our major activity at the moment is side-channel analysis, which is a major topic in smart card industry. So there are attacks where you measure the current and try to get some secret about the key from the current measurements. This will also be a topic for RFID tags. And we are doing projects with quantum groups.

And yeah, this is-- what makes us so special is probably the strong interaction with the other groups we have at our institute. Especially when developing AES, it was very helpful to have Vincent Rijmen sitting with us together to find out how we can serialize the algorithm to comply with the requirements we have in RFID.

So we talked a lot about that already. I will skip that slide because Sanjay today in the morning all explained this. So there is actually a need for security. And we say if you put security on a tag or on RFID, you should use proper security, so lightweight security. In our sense, it's not lightweight crypto, so lightweight implementation of real crypto, because if you try to get in with security in a globalized technology, you will need standardization. And that prevents, of course, secrets in the algorithm.

So the standardized algorithms like AES, RSA, ECC, they are approved by experts. So there is some work spent in investigations if they are secure. And if you do not use them, you're probable to flaws in your systems. And the thing is you should not only look at the algorithms you use. Most [INAUDIBLE] systems get broken because they do not use standardized protocols, so most flaws in systems are in protocols.

And now I want to bring some arguments against and for standardized algorithms. So some people say that if you use standardized algorithms, they are easy to attack because there are so many publications on attacks. And you do not take into account that your developers of the system. And if you're talking about RFID, there are a lot of developers. They are potentially attackers. The secret is not a secret if so many people got involved.

And some people say that especially side-channel analysis is more dangerous if the algorithms are known and if the RFID tag are in the hands of the attackers, and they are in the hands of the attackers, I would apply a side-channel attack. And if you understand side-channel attacks, it's easy to adopt them to other algorithms. It's also easier to use them to find out the specifics of secret algorithms. So that's not a question.

And some people say that custom-built algorithms use less secure. You lose less resources. And I say that they are potentially less secure. If you use them, things might happen. Like, it was exactly last year, I think, this break of the John Hopkins [INAUDIBLE] of the [? speed pass. ?] And we say that proper implementations of standardized algorithms are possible for passive devices, for RFID tags. And I will show you later on our modules.

So when we started, we defined some requirements for secure tags we wanted to develop. And we said right from the start we do not want lightweight crypto. We want real crypto, like the same standard as in smart card industry.

We wanted to use standardized algorithms, because the high number of tags we will have is enough value that even if each tag just protects small value, it's a good point of attack for an attacker because the high number of tags makes a hack very interesting. But the high number of tags logically needs a very clever key management. So we do not have systems like that so far.

We didn't want to accept a raise of costs, a significant raise of costs, due to our security implementations we wanted to have on the tags. And we didn't want to accept a reduction in reading distance. So we had to comply with this very small power consumption. And we wanted to be compatible with our already installed infrastructures. So we didn't want to suggest a system which is never accepted because there are so many readers already out there.

And there we started, and then we were facing a lot of limitations due to the technology. So the main problem is the power consumption. So if we do not accept a reduction in the reading distance, we were facing that we have about 10 microamps available. The area consumption, which is less problem with new semiconductor technology, but it's still the technology that's now available.

We have very limited execution time, in fact, because, well, we have a rather limited clock frequency. So the protocols, that was actually a problem, because in the other things, you can say just a client, and the server client just responds or something like that. But here always the protocol is always initiated by the reader, and that's different. And there is no physical protection available possible.

And then there were a lot of publications in the last year where people state that hash is more inexpensive that the encryption, and that's simply not true. So I do not say that this research is useless, but they should use encryption modules instead of hash models because they are easier to implement in hardware.

So what are the enhancements we want to propose? For tag identification, we will need an extended personalization. We will need a crypto, primitive, on a tag. And we will need to secure key storage on a tag, which is a problem that is not treated so far. And we need the cryptocapability of the reader or a secure access to a verification server.

For read authentication, we will need one additional thing. That's nonce generation. Nonce a number used once. It's kind of pseudo-random number. It has to be fresh and unpredictable, and that's not an easy task for RFID tags.

What are the results so far? In our institute, we developed an AES module, which complies with the requirements for a tag. So it uses 4.5 microwatts. That's produced. That's verified. That's available. The only thing is there is no countermeasures against side-channel attacks on this module. That's what we are working on so far.

We presented security layers for ISO 18000. The reason why we've chosen this standard is because we were used to the ISO standards from smart card, and it was, when we started, clearer to us the concept of defining new comments like this, custom comments, which were foreseen in ISO 18000. In fact, it doesn't make a big difference if we use EPC or ISO.

We have protocol security layers for anti-cloning, for privacy enhancement. And this is tested with a tag emulator and FPGA basis. And we have isometric crypto modules using elliptic curve cryptography, which are usable on passive devices.

So what are our future task? We will work on-- we should work, actually, on key management and personalization, on testability of crypto tags. Nobody mentioned that so far. This will be a problem in future. So if there is more functionality in tags, how will you test them? Compliance testing is already a topic, but this will be a more interesting topic. We have to deal with this nonce generational tag and further research on isometric crypto.

So what are the conclusions? Use standardized crypto if you state that you will. Design secure RFID systems, because you never know what your system is used for then. The protection will be also necessary in inexpensive tags in future because you never know the applications, also protection against side-channel analysis.

And, well, according our results so far, I would say the implementation of standardized crypto is possible on passive devices if you go for a clever implementation. And more research is definitely necessary for integration into running applications, to future applications. This is a list of our recent papers.

And I just want to mention our initiative, PROACT. We are looking for research, for professorship, and for visiting professors, and stronger interaction with the RFID community in the next years. And thank you.

[APPLAUSE]

STEVE MILES: Any questions for this distinguished panel around just the tags and the future of tags? If we could ask you to come down to the mics.

AUDIENCE: This is Chris [INAUDIBLE] from the Auto-ID Lab in Switzerland. I have just a quick question regarding your work on power consumption reduction. If you look at the works, say, of [INAUDIBLE] on transponders, their transponders needed about 16 microwatts at the antenna and probably about 4 microwatts on the chip before the rectifier. Where do you think your work will take this? Do you think you can get significantly, be 1 microwatt, for power consumption of a tag for read access?

HAO MIN: Actually, your question is-- you will see that the minimum power for the tags, there's IF power. Say it's, like, 16 microwatts. But the real digital power consumption is, like, a 4 watt. So this means that there's only 20% of the microwave power was converted into DC power.

So our work is-- we can get the performance better by doing two things. One is we can improve the conversion rate, which is higher efficiency to convert the microwave power into DC power. The second thing is that by carefully designing so the digital circuitry would reduce the power consumption. So this is a two-way, where each go together to reduce the power consumption. But eventually, what decides the read range is the IF power, decides the whole read range.

AUDIENCE: But what do you think this is moving to? We you see that at some point we will be down to, like, 1 microwatts?

HAO MIN: I think probably even less than 1 microwatts. Yeah. Just like in [INAUDIBLE] stations, if we use some special circuitry, we even can reduce the power consumption by a factor of 10, even 100. We take advantage of that the tag really work in really low operating speed.

So for the maximal-- the clock in a gen 2, it's only a 640k, which is much-- even 1,000 times slower than a PC is working. So probably, it's just can use some special circuitry. You can reduce the power of that to, like, a 100 times. Then [INAUDIBLE].

AUDIENCE: OK. Thanks very much.

HAO MIN: OK.

STEVE MILES: So thank you very much. If we could ask the next panel to come up, in the interest of time.