Securing RFID with Ultra-wideband Modulation

Pengyuan Yu, Patrick Schaumont and Dong Ha

Virginia Tech
Electrical and Computer Engineering Department.
Blacksburg, VA 24061

Abstract. Current implementations of secure RFID rely on digital cryptographic primitives in the form of hashes and block ciphers. The presence of these blocks is motivated by privacy requirements, but they increase the overall processing latency, the power consumption, and the silicon area budget of the RFID tag. In addition, existing passive RFID systems rely on simple coding and modulation schemes using narrowband radio frequencies, which can be easily eavesdropped or jammed. We propose to implement the link from RFID to reader using ultra-wideband (UWB) communications. We show that the use of an advanced modulation scheme offers a new approach to the secure RFID problem. By using the modulation spreading code as a secret parameter of the communications link, we can make eavesdropping extremely difficult and increase the communication reliability. We also show that it decreases the latency and the risk for side-channel attacks. We present the digital baseband architecture of a passive UWB-RFID that uses time-hopped pulse-position modulation (TH-PPM), and present area- and power estimates that are competitive to solutions using digital cryptography.

1. Introduction

Passive RFID capture and reuse incoming radio-frequencies to power internal circuitry and to respond back to the RFID reader. The available RF power of the reader-transponder system is constrained at both sides of the link, either by regulations or else by technological limits. A typical example of an UHF (900 MHz) tag enables a power budget of 150 μW for a tag located at 2 meters from a reader that uses a 500mW transmitter [1]. Current systems implement a half-duplex link between reader and tag. The reader sends a power-carrying RF carrier to the tag, adding additional data by means of amplitude modulation. The reverse link, from tag to reader, is based on adaptive reflection (backscatter) of the phase of the incoming RF carrier, or on adaptive loading [2]. In both directions a narrowband signal is used, with a bandwidth much smaller than the carrier frequency. These communication schemes have been developed with simplicity in mind. They are susceptible to passive attacks such as eavesdropping [3][4][8] and active attacks [5].

In recent years, many proposals have been made to address the privacy issues related to such tags, as well to extend their application domain to include authentication besides detection [6,10,12,13]. All of these proposals are enhancements at either the protocol-level or else at the algorithm-level of the communications link.

They make the implicit assumption that the communications link between tag and reader can be eavesdropped and thus that privacy must be guaranteed by the data link layer. Many of these proposals rely on digital block ciphers or hashes. Indeed it has been shown that traditional digital cryptography can be implemented within typical implementation constraints of passive tags. Feldhofer presents an implementation of AES of 3595 equivalent NAND gates that consumes 8.5 μA [6]. This shows that symmetric-key implementations can meet area and power constraints of tags. A similar conclusion, made for the case of low-frequency tags (13.56MHz), can be found in [7]. However, the use of digital cryptography in a power- and silicon-area-constrained context is not without cost. The presence of digital ciphers in RFID tags increases their response-time. A high cycle count budget combined with a low operation frequency results in substantial computation times for these ciphers. For example, the AES implementation discussed in [6] requires 995 cycles. At a tag clock frequency of 1MHz, this implies that one round of encryption will take close to one millisecond. The new Gen-2 tags take 1.6 milliseconds to transmit a 128-bit tag [9]. Consequently, the tag encryption time therefore is of the same order of magnitude as the transmission time of the encrypted result. This latency reduces overall system throughput and in some cases violates the constraints of the standard [6]. In addition, the tag computation and communication will be clearly separated in time, making it easier to mount a power-analysis side-channel attack that focuses on the cipher [8].

Recent work in so-called 'light-weight' protocols tries to alleviate the requirements of encryption or even eliminating them altogether. The HB+ protocol, for example, uses a protocol modeled after human authentication [10]. It uses repeated challenges directly derived from the shared key K. Unfortunately the HB+ protocol was not resistant against active attacks [11] Besides HB+, several good proposals have been presented recently, all of which use a cryptographic primitive (hash function or cipher). The hash-lock scheme from Sarma and Weis [12] uses the concept of a lock based on hash-functions. The YA-TRAP protocol from Tsudik [13] relies on time-stamping RFIDs and a hash function to prevent unauthorized tracking. So far, there does not seem to be 'an easy way out' that will make cryptographic primitives in authentication protocols obsolete.

What we rather need is a significantly more efficient implementation of those secure protocols. To this end, we propose to secure physical communications based on ultra-wideband modulation (UWB) and time-hopping. Rather than encrypting the tags' identifier, we use a private modulation code. This modulation code changes for each bit that is transmitted from the tag to the reader. Only a receiver who knows the sequence of modulation codes will be able to receive the overall message. Our approach offers the following benefits over current secure RFID tags.

- UWB transmissions are very hard to eavesdrop because of their large bandwidth.
- Secure-UWB modulations can use simple ciphers. We will show that eavesdropping on a 16-bit secret modulation code already requires high-end communications equipment.
- Secure-UWB tags have low latency, and are able to respond much faster to a reader because each data bit is secure-modulated separately.

- UWB transmissions are more robust to interference than narrowband transmissions. They are difficult to jam and allow concurrent transmissions in the same band.

In this paper, we present our initial results in the design of a digital baseband for an UWB RFID tag. In Section 2, we will first briefly review the properties of ultra-wideband modulation, and discuss our proposed time-hopped pulse-position modulation. We will also present the communications protocol between a tag and a reader, and summarize the security risks of our approach. In Section 3, we present the details of a digital baseband architecture for our tag. This includes a discussion of the modulation-code generator, as well as a discussion of a pulse-position modulator that drives the UWB front-end. We will present estimates for timing, area, and power for an implementation in 0.18 micron CMOS technology. In section 4, we summarize and conclude the paper, and point out future plans and open research issues.

2. Ultra-Wideband RFID

2.1 Low data-rate and low-cost UWB communications

Since the FCC's allocation of a UWB spectrum in the range of 3.1 GHz to 10.6 GHz in 2002, UWB has gained phenomenal interest in academia and industry [14]. Compared to traditional narrowband communication systems, UWB has several advantages including high data-rate, low average radiated power, and simple RF circuitry. Many of these potential advantages are a direct consequence of UWB's large instantaneous bandwidth. Shannon's theorem states that the channel capacity C is given as $B.log_2(1+SNR)$, where B is the bandwidth and SNR is the signal-to-noise ratio [15]. As the bandwidth B is much larger (on the order of several GHz) for UWB than for a narrowband signal, the SNR can be much smaller for UWB to achieve the same data rate. Therefore, UWB is often able to recover data, even if the signal power is close to the noise level. In other words, the presence of UWB signals is harder to detect than narrowband signals.

The IEEE 802.15 WPAN task group has recognized the potential of UWB for low data rate applications, and is in the process of standardizing the physical layer [16]. Hancke and Kuhn presented a paper on securing RFIDs using UWB, to the best of our knowledge, the only one so far on this topic [17]. They suggested measuring the signal propagation delay between an RFID and the reader using UWB. If the delay exceeds a certain bound, the system signals a possible attack.

UWB signaling can be carrier-based or impulse-based, and impulse-based UWB is more suitable for the RFID due to its simple hardware. Impulse-based UWB is based on a train of narrow pulses (which are typically a few tens to hundreds picoseconds wide). Various modulation schemes such as on-off keying, pulse amplitude modulation, pulse position modulation (PPM), and binary phase shift keying are available for UWB. A binary PPM scheme has 2 distinctive time positions in a time slot, and one pulse carries 1 bit of information. We adopt PPM due to its low

hardware complexity [18]. A k-bit time hopping PPM (TH-PPM) allocates 2^k time slots for each bit and hops time slots between pulses. Figure 1(a) shows an example TH-PPM scheme with four time slots in each cycle. The first pulse occupies the second time slot, the second pulse the first slot, and the third pulse the fourth slot in the figure. Like any other PPM, the position of a pulse within a time slot carries the information bit for TH-PPM. For example, a pulse aligned to the start of a slot represents logic 0 (Figure 1(b)). A pulse delayed by Δ with respect to the start of a time slot carries logic 1 (Figure 1(c)).

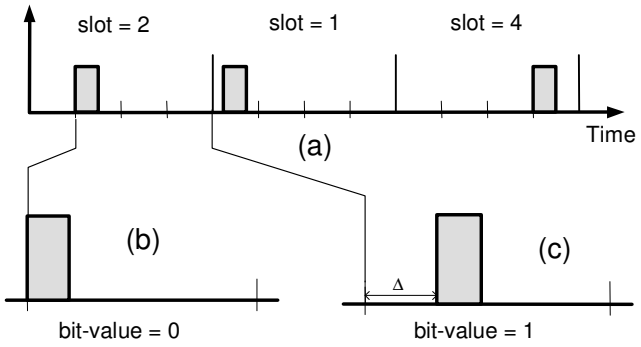

Figure 1: Time-Hopped Pulse-Position Modulation (TH-PPM)

So far, time-hopping has been used in communications for two purposes; multiple access and/or spreading of the spectrum. We introduce a new application of time-hopping, which is to secure physical layer communications through time-hopping. This is possible because of the following. To demodulate extremely narrow UWB pulses, a receiver should correlate incoming pulse signals with a template signal. The time slot of an incoming pulse is known a priori for a conventional TH-PPM scheme. The receiver performs two correlations starting at two different instances, one at t=0 as for the case in Figure 1(b) expecting a logic value 0 for the incoming signal and the other at t=Δ as in Figure 1(c) expecting logic 1. One of the two correlation operations will capture the received signal energy, while the other one will only correlate noise. If the time slots of pulses are assigned in a pseudo random manner, the eavesdropper should perform correlations for all possible time slots. If the total number of time slots is sufficiently large and each time slot is sufficient small, eavesdropping of TH-PPM communications is practically impossible.

2.2 UWB frame format for RFID

We now discuss the data framing for our secure RFID system. We start our discussion with the basic transmission frame format, followed by a security analysis.

Figure 2 illustrates a frame for the transmission of a single ID. The transmission needs to complete within 10 ms, similar to present-day non-secure RFIDs. The frame

contains a 2ms preamble and an 8ms data-field. The preamble contains 32 known bits at the same time slot within each cycle. The purpose of the preamble is to synchronize the reader. Next, a pulse train of 128 bits follows. Each bit uses a different pseudorandom time slot. The cycle time, i.e., time window of a single bit, is 62.5 μs. The system in Figure 2 uses a 16-bit pulse-position code, resulting in 2^{16} (=65,536) time slots, each slot being 954 ps long. This slot length is long enough for a UWB pulse not to interfere with the pulse from the next time slot.

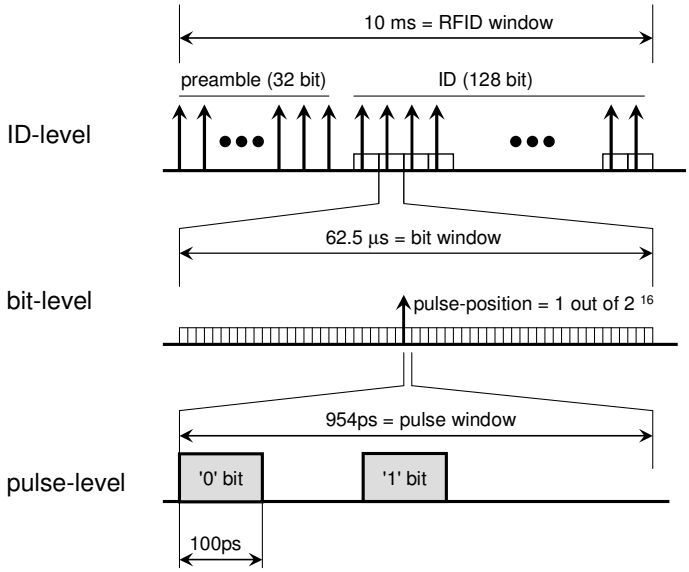

Figure 2: Frame format for tag-to-reader communications

Next we consider the cost of eavesdropping (passive attack) or jamming (active attack) this transmission. First, consider the case of eavesdropping. Suppose that an attacker successfully synchronizes his/her reader (or a UWB receiver) using the preamble. A brute-force attack is to capture every signal within the remaining 8 ms transmission window of an RFID. To capture enough energy for each pulse with duration of 100 ps, at least ten samples are required per pulse. This requires about 168 Msamples per 8 ms period (which is 20 samples for each time slot, for 65,536 slots per bit and 128 bit for the entire read cycle) – this is a very expensive measurement in terms of complexity and instrumentation cost. More importantly, the ADC (analog-to-digital converter) used to sample these pulses should operate at the sampling rate of 100 Gsamples per second, which is not feasible for current technologies.

An alternative strategy would be to attack a certain fixed time slot, for example, always to read the first slot of each cycle, and perform multiple RFID read operations until each pulse of 128 bits hits the time slot at least once. This would need, on average, 65,536 / 2 read operations for the example shown in Figure 2. We can thwart this attack by deactivating the RFID automatically after a certain number of reads, defined by its expected lifetime (presumably smaller than 65,536 / 2 reads). In our

implementation, we used a different approach. We XORed the ID data-bits with bits taken from the pseudorandom stream that feeds the time-slot selection.

Active attacks, using jamming, are complex to implement as well. This requires disruption of the signal exactly at the position where an UWB pulse is located, and hence requires knowledge of the modulation code. If the objective would be only to jam the signal, a transmitter should generate a distortion pulse at each possible pulse position. This requires a significant amount of transmission power in the GHz range, which is very expensive in hardware. Therefore, while it is not possible to claim that secure UWB will perfectly resist attacks, we can reasonably assume that they are difficult to mount. In addition, the eavesdropping protection offered by UWB is much cheaper in hardware and is complementary to traditional cryptography used in RFIDs.

In the next section, we discuss the overall architecture of a tag that uses the UWB scheme discussed above, and we provide details on the digital baseband implementation.

3. Architecture of an Ultra-Wideband RFID

In this section we present an overview of the UWB-RFID tag architecture, including design details of the digital baseband parts.

3.1 UWB-RFID tag architecture

Figure 3 illustrates the architecture of our UWB-RFID tag. There are two front-ends in the tag: a narrowband receiver front-end and an UWB transmitter front-end. The narrowband receiver front-end is responsible for reader-tag communication and for power extraction. It is similar to that of existing tags and will not be discussed further. The ultra-wideband transmitter front-end generates a narrow pulse on the order of 100ps. The pulse location is defined with a pulse-position modulator (PPM). The PPM creates a step-function with the step located at the desired pulse position (edge input). The pulse bit value is defined by the actual data bit to be transmitted (data input). Because of the very low duty cycle of the UWB pulses, the transmitter can be constructed within the power budget available to passive RFID tags. For example, [16] presents a transmitter design that delivers a 40MHz UWB pulse rate with 2mW of power. The pulse rate that we defined in Figure 2 (16KHz) is more than three orders of magnitude lower than that, which will push power consumption in the μW range. In this paper we will not elaborate further on the UWB front-end.

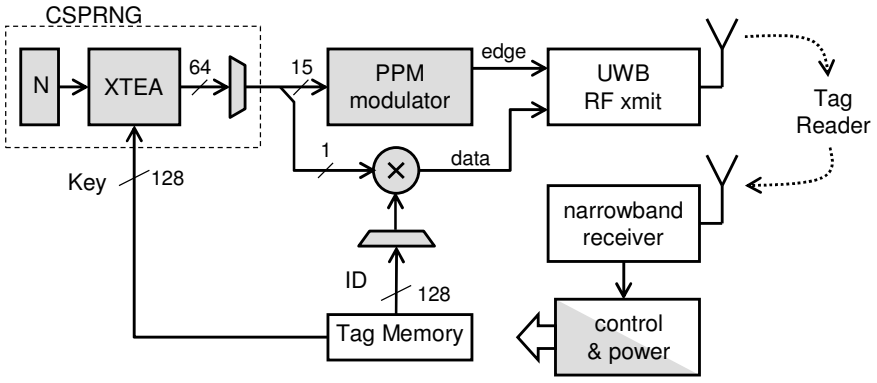

Figure 3: System architecture of a passive UWB RFID Tag

The digital baseband generates a pulse-position modulated signal for the UWB frontend. The pulse positions are selected by means of a cryptographically secure pseudo-random number generator (CSPRNG). Since the CSPRNG is used to select the modulation code rather than for strong encryption, we can opt for a simple block cipher operating in output feedback (OFB) mode, which provides less area and cycle count overhead when compared with strong cipher such as AES.

For the framing format defined in Figure 2, a 16-bit block cipher would have been adequate. Since no standard ciphers are available with this block-length, we selected instead an existing 64-bit cipher (XTEA) and used the output of each encryption round for four subsequent UWB pulse-positions. The most significant bit of each number of the pseudo-random sequence is used to encrypt the data bit. This is done to circumvent an eavesdropping attack on a fixed timeslot. Note that we only used 15 bits to select the timeslot, i.e., in our current implementation we position UWB pulse over only half the range of a 62.5 µs timeslot. We will show that this considerably relaxes the timing constraints on the baseband implementation, and it limits the peak power consumption of the UWB front-end.

In the following, we will discuss the operation and implementation of the CSPRNG and of the pulse-position modulator. Next, we will discuss several aspects related to the system timing, and propose a reader-tag communication protocol to synchronize the CSPRNG.

3.2 Pseudorandom number generator

The pseudorandom number generator is based on a simple block cipher in output-feedback mode. The key of the block cipher is a predetermined secret between the tag and the reader. A counter N is used as the initialization vector for the output feedback mode. The counter is incremented after each RFID read operation. We used a 64-bit XTEA algorithm [20] which requires 32 rounds per 64 bits. To reduce hardware area,

we mapped only half of the operations of the XTEA data processing as illustrated in Figure 5. The other half can be obtained based on the Feistel symmetry of XTEA. The cipher therefore produces 64 pseudorandom bits in 64 clock cycles.

The pseudorandom bits are consumed in groups of 16 bits by the PPM modulator and the data xor operation (Figure 3). As each bit is transmitted in a 62.5 µs window, this implies that the XTEA algorithm must run at 256 KHz.

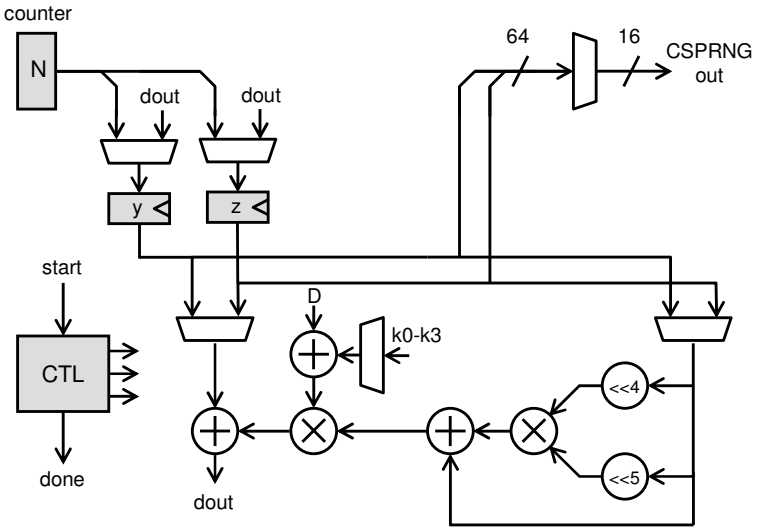

Figure 5: CSPRNG based on ½ XTEA in counter mode

3.3 Pulse-position modulator

The purpose of the pulse-position modulator is to generate precise time delays and communicate the location of UWB pulses to the UWB front-end transmitter. Within a 62.5 µs time window, the PPM has to implement a resolution of 2^{16} time steps, which corresponds to 954ps per step. This resolution prohibits us to use a counter-based approach in generating the delays, since the counter would have to be run at 1.048GHz.

Figure 4 shows a distributed solution to delay generation. Each stage of the PPM chain implements a single bit of delay, equal to either one or two clock periods of that stage. In addition, each stage generates a divided clock for the next (earlier) stage. The delay contribution of each stage will thus increase in powers of 2. This way, the design minimizes the number of registers that run at high clock speed. We opted to introduce at least one period of delay per stage since this enables us to pipeline the entire pulse-position modulator. The complete chain includes 15 stages, which have clocks from 1.048GHz to 64 KHz.

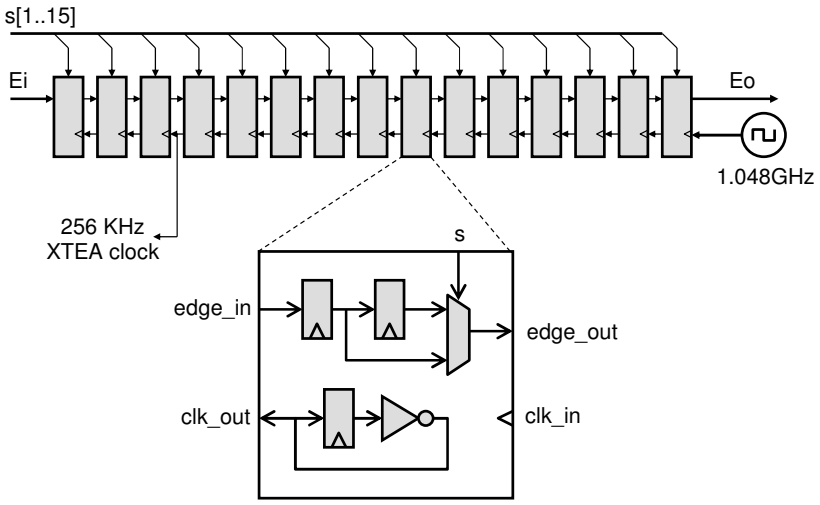

Figure 4: 15-bit Pulse Position Modulator with 1ns resolution

The delay generated by the PPM is defined in terms of a 15-bit input number S:

$$\Delta = C\left(1 + \frac{S}{2^{15}}\right) \qquad (1)$$

$$C = 31.25\mu s - 954\,ps$$

Figure 5 shows the relationship between the input and output signals of the PPM. The input signal is a 15.625 µs pulse created by the controller. The delay chain delays this signal between a half and a full bit window based on the delay parameter S. Therefore, two subsequent UWB pulses will always be separated at least half a bit window apart, and the immediate UWB pulse rate cannot exceed 32 KHz. This limits the peak power consumption of the UWB front-end.

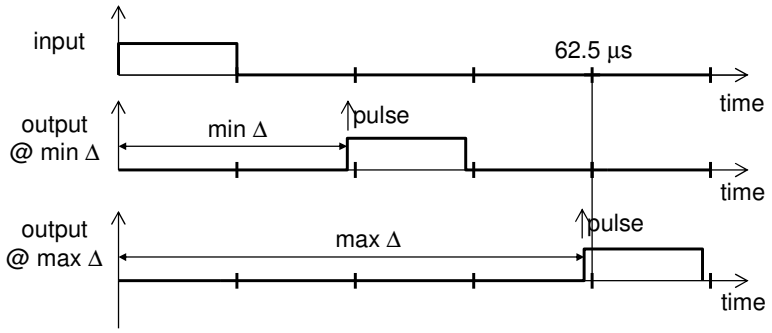

Figure 5: Time relations of input/output signals in the PPM.

3.4 Implementation results

We implemented the shaded areas of Figure 3, corresponding to the digital baseband of the tag, into 0.18 µm CMOS to obtain gate-count, area, timing, and power consumption estimates. The present implementation uses 4636 gates, and has hard-coded constants for the tag key and the tag ID. The power consumption was obtained using Synopsys Power Compiler under typical conditions, with back-annotated net activity results obtained from simulation. The results are shown in Table 1. Note that the bulk of the power is consumed in the front-end stage of the PPM (U0), and is caused by the high clock frequency of that stage. Thus, if we would decrease the PPM resolution by a single bit, power consumption would decrease by half. For such a reduced PPM resolution, the effort of an eavesdropping attack is still very high (42 Msamples captured at 50 Gsample/s). We are presently pursuing further research on the system parameters, and expect to be able to reduce the power consumption considerably.

Table 1: Implementation Complexity of UWB Digital Baseband for RFID

			Power		**Gate Count**	**Clock Period**
			Absolute (µW)	Relative		
RFID Tag Digital Backend	**CSPRNG**		14.8	2.1 %	3264	2^{12} ns
	DELAY CHAIN	U0	298	41.5 %	382	2^{0} ns
		U1	147.4	20.5 %		2^{1} ns
		U2	73.8	10.3 %		2^{2} ns
		U3	36.8	5.1 %		2^{3} ns
		U4	18.4	2.6 %		2^{4} ns
		U5	9.2	1.3 %		2^{5} ns
		U6	4.6	0.6 %		2^{6} ns
		U7	2.3	0.3 %		2^{7} ns
		U8	1.16	0.2 %		2^{8} ns
		U9	0.58	0.1 %		2^{9} ns
		U10	0.30	0.0 %		2^{10} ns
		U11	0.33	0.0 %		2^{11} ns
		U12	0.11	0.0 %		2^{12} ns
		U13	0.04	0.0 %		2^{13} ns
		U14	0.02	0.0 %		2^{14} ns
	CONTROL		41.2	5.7 %	990	2^{12} ns
OVERALL			**718**	**100 %**	**4636**	**N/A**

3.5 System synchronization protocol

In the design described above, we assumed that the reader CSPRNG is synchronized to the tag CSPRNG. However, the protocol described earlier can be extended easily to include this synchronization. At the start of the scanning process,

the tag first sends the iteration count N of the XTEA counter. This N is transmitted without time-hopping, and can for example be included as part of the preamble as shown in Figure 6. After the default preamble of 32 bits, the tag transmits the 64-bit value of the counter with a fixed pulse-position. Next, it sends a new preamble to enable the reader to synchronize the local CSPRNG. After that, the actual ID can be transmitted.

The value of N is thus not protected from eavesdropping, yet it is of limited value to an attacker. The actual time-hopping sequence is determined by both N and the XTEA key. This key remains a system-wide secret for all tags associated with a reader.

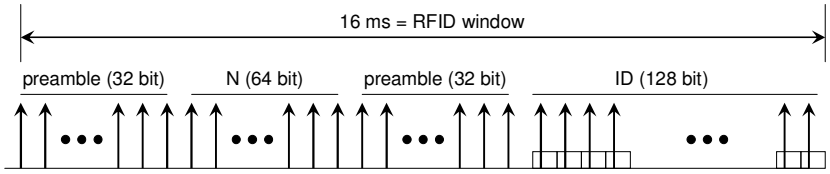

Figure 6: UWB frame with counter synchronization

4. Conclusions and Future Work

We have proposed the use of UWB communications to implement secure RFID. Instead of encrypting data, we focus on making the communications difficult to eavesdrop. Our first results show that the system is technically feasible and a valid alternative to solutions based on narrowband communications. We are presently refining our concept and the system parameters. We are also considering how UWB can be used to cover other RFID applications as well. In particular, the multi-access properties of UWB will be useful to define more efficient approaches to the time-consuming singulation process of present RFID systems. Second, UWB has better propagation properties than traditional narrowband communications. We thus envisage UWB RFID to be useful in environments that are unsuited for small-band tags.

5. Acknowledgements

The authors acknowledge the support of ST Microelectronics.

6. References

1. U. Karthaus, M. Fischer, “Fully Integrated Passive UHF RFID Transponder IC With 16.7-μW Minimum RF Input Power,” IEEE Transactions on Solid-State Circuits, 38(10):1602-1608, October 2003.

2. K. Finkenzeller, “RFID Handbook: Radio Frequency Identification Fundamentals and Applications,” Chapter 4 – Physical Principles of RFID Systems, John Wiley & Sons, 1999.
3. I. Kirshenbaum, A. Wool, “How to build a low-cost, extended-range RFID skimmer,” IACR eprint architecture 2006/054, online at http://eprint.iacr.org/2006/054.pdf.
4. K. Mahaffey, M. McGovern, P. Simmonds, J. Callas, “Long Range RFID and its Security Implications,” presentation at BlackHat USA 2005, Las Vegas.
5. L. Grunwald, “RFID and Smart Labels: Myths, Technology, and Hacks,” BlackHat USA 2004, Las Vegas, July 2004.
6. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, “Strong authentication of RFID systems using the AES Algorithm,” Proc. of the 2004 Cryptographic Hardware and Embedded Systems workshop (CHES 2004), LNCS 3156, p 357-370, 2004.
7. T. Lohmann, M. Schneider, C. Ruland, “Analysis of Power Constraints for Cryptographic Algorithms in Mid-Cost RFID Tags,” Seventh Smart Card Research and Advanced Application IFIP Conference (CARDIS 2006), LNCS 3928, p 278-288, 2006.
8. Y. Oren, A. Shamir, “Power analysis of RFID tags,” online at http://www.wisdom.weizmann.ac.il/~yossio/rfid/.
9. AutoID Center, “Draft protocol specification for a 900 MHz Class 0 Radio Frequency Identification Tag,” February 2003.
10. A. Juels, S. Weis, “Authenticating Pervasive Devices with Human Protocols,” 25th Annual Cryptology Conference (CRYPTO05), August 2005, Santa Barbara, CA.
11. H. Gilbert, M. Robshaw, and H. Sibert, “An Active Attack Against HB+ - A Provably Secure Lightweight Authentication Protocol”, Cryptology ePrint Archive 2005, publication 237, online at http://eprint.iacr.org/2005/237.pdf
12. S. Sarma, S. Weis, and D. Engels, “RFID systems and security and privacy implications,” Proceedings of the 2002 Cryptographic Hardware and Embedded Systems Workshop (CHES02), LNCS 2523, pp. 454--469, Springer, 2002.
13. Gene Tsudik, “YA-TRAP: Yet Another Trivial RFID Authentication Protocol,” Proceedings of the International Conference on Pervasive Computing and Communications, PerCom 2006.
14. J.H. Reed (editor), “An Introduction to Ultra Wideband Communication Systems,” Prentice Hall, 2005.
15. J. G. Proakis, “Digital Communications,” McGraw-Hill, 1995, xxi+928 pages.
16. IEEE 802.15 WPAN Low Rate Alternative PHY Task Group 4a, online at http://www.ieee802.org/15/pub/TG4a.html.
17. G P. Hancke and Markus G. Kuhn “An RFID Distance Bounding Protocol,” Proceedings of SecureComm, pp. 67–73, 5–9 September 2005.
18. K. Marsden, H.-J. Lee, D.S. Ha, and H.-S. Lee, “Low Power CMOS Re-programmable Pulse Generator for UWB Systems,” IEEE Conference on Ultra Wideband Systems and Technologies, pp. 443-447, November 2003.
19. J. Ryckaert, C. Desset, A. Fort, M. Badaroglu, V. De Heyn, P. Wambacq, G. Van der Plas, S. Donnay, B. Van Poucky, B. Gyselinckx, “Ultra-wideband Transmitter for Low-power Wireless Body Area Networks: Design and Evaluation,” IEEE Trans on Circuits and Systems-I:Regular Papers, 52(12):2515-2525, December 2005.
20. R. M. Needham, D. J. Wheeler, “Tea extensions,” Technical report, Computer Laboratory, University of Cambridge, October 1997.