

# Securing RFID with Ultra-wideband Modulation

Pengyuan Yu, Patrick Schaumont and Dong Ha



Center for Embedded Systems for Critical Applications

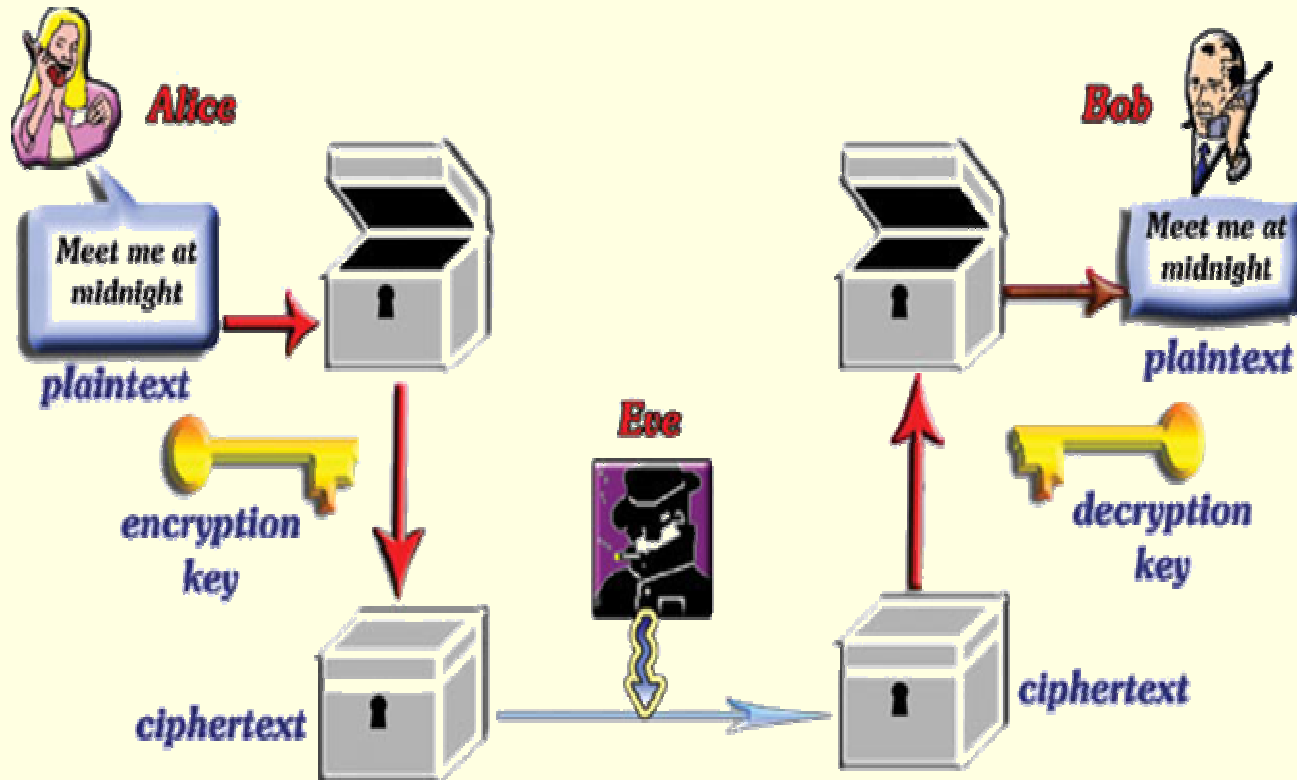
Presented By: Eric Simpson

# Summary

---

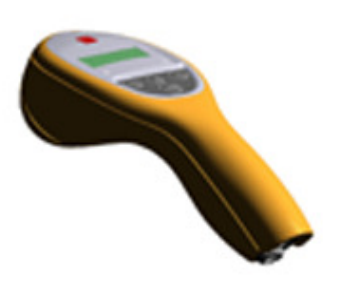
- Traditional Secure Communications
- Securing the physical layer with UWB TH-PPM
- RFID digital baseband implementation

# Traditional Encrypted Channel



**Assumption:** Eve can intercept and store transmitted data

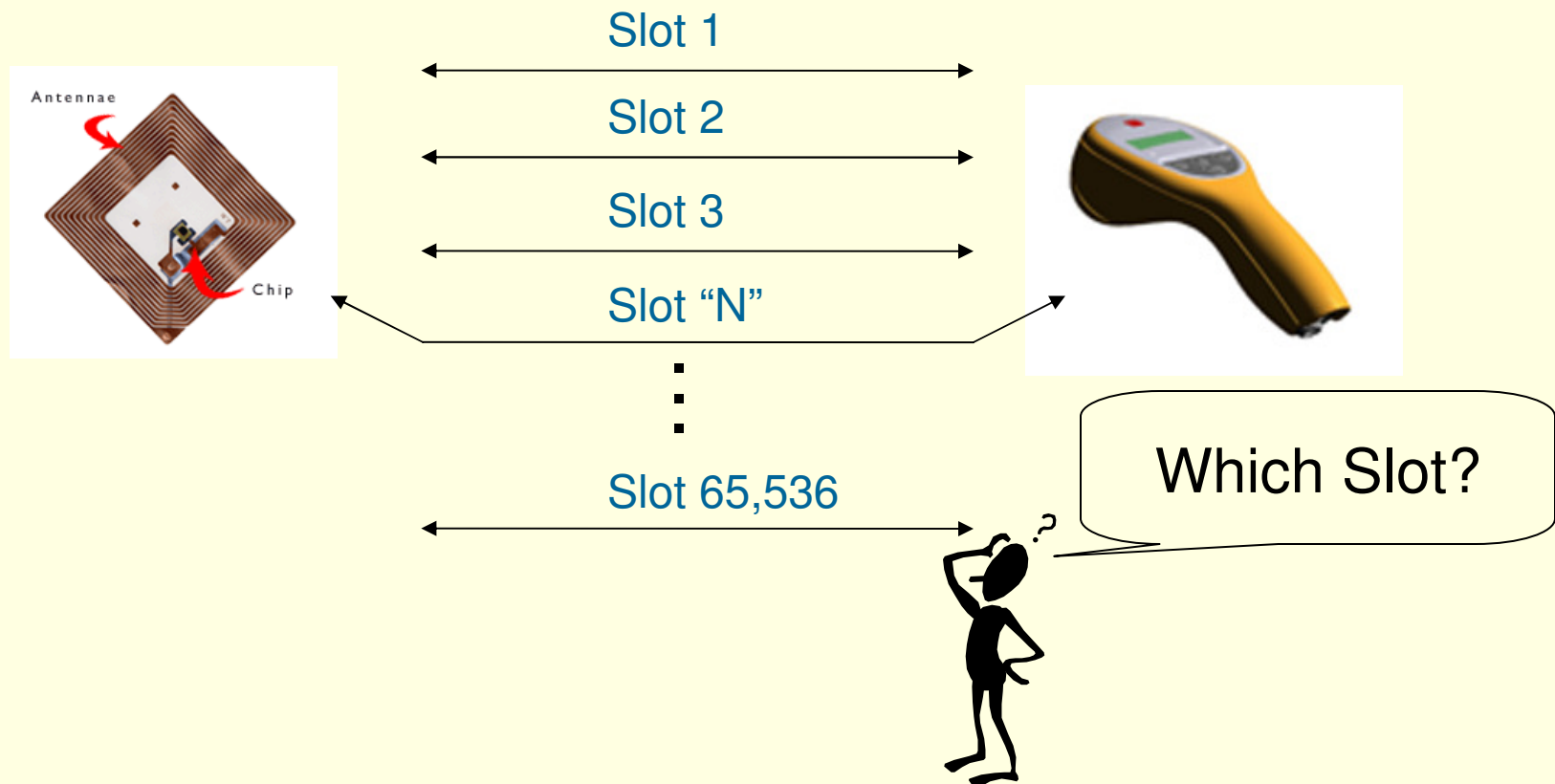
# Insecure Physical Layer with Narrowband Signals



- Requires **computationally** secure cryptography
  - Still must meet area, power and latency constraints of an RFID tag
- Use of light-weight protocols

# Our Approach – Secure Physical Layer

- Goal: Secure data by making interception of the data infeasible.

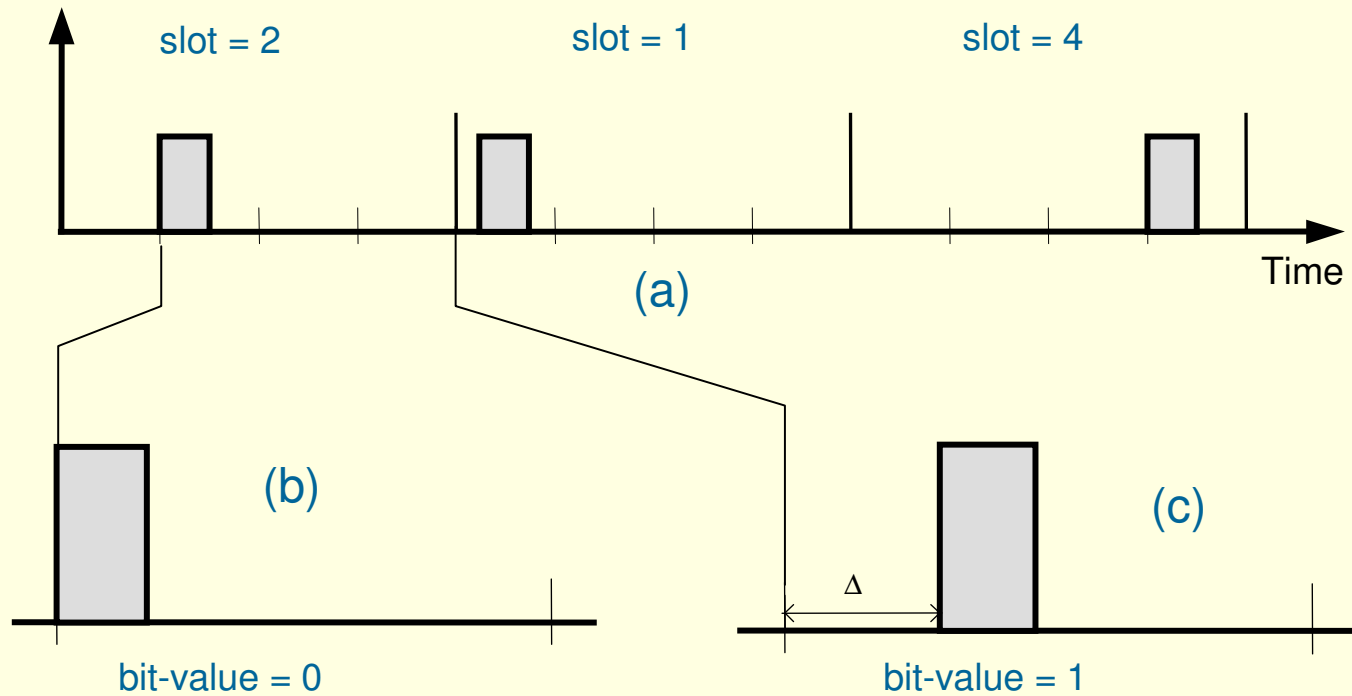


# Benefits of UWB TH-PPM

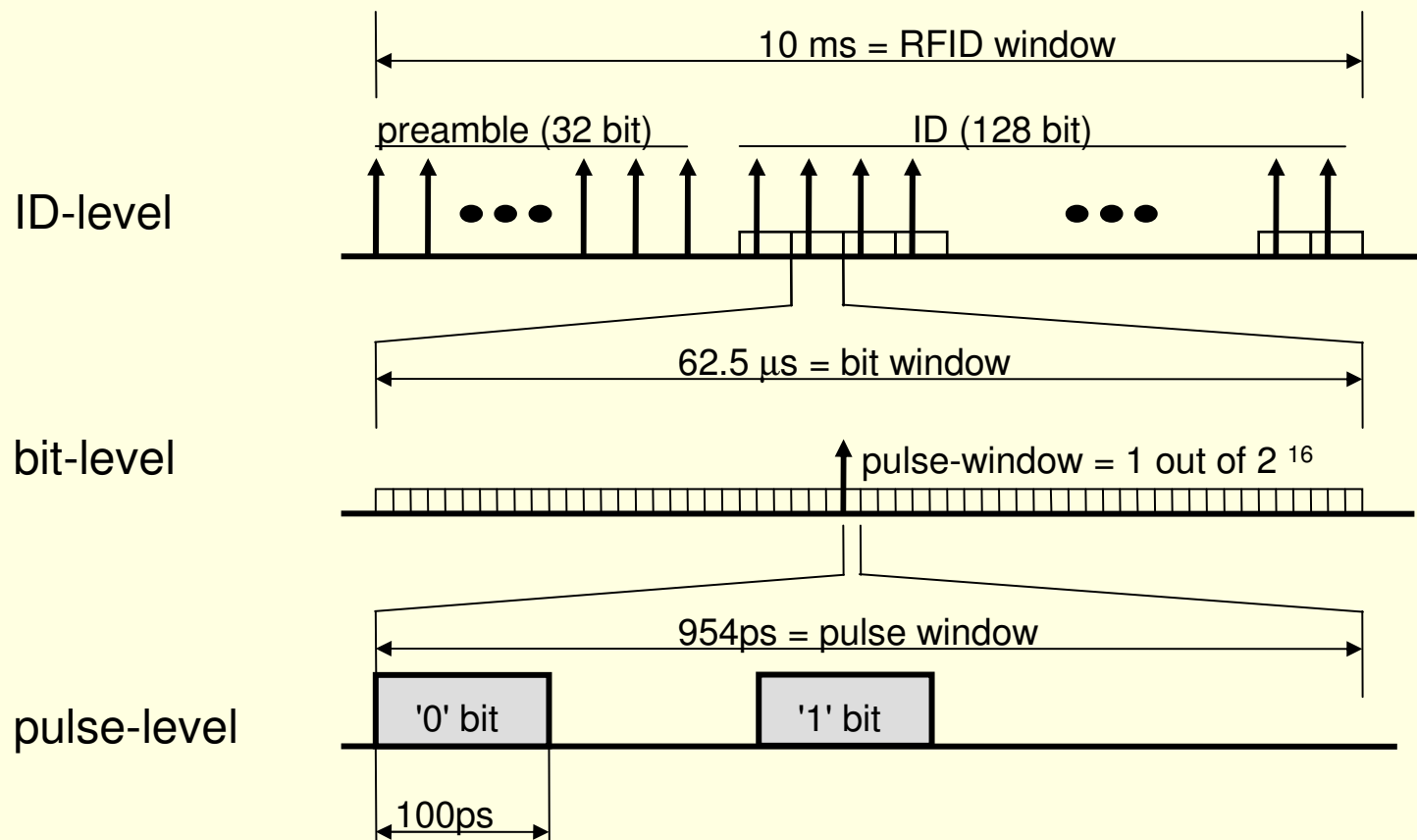
---

- Can use simple ciphers
  - 16-bit secret modulation code requires high-end communications equipment
- Low Latency
- UWB is more robust to interference than narrowband
- Allow multiple concurrent transmissions in same band

# TH-PPM



# UWB RFID Tag Frame Format

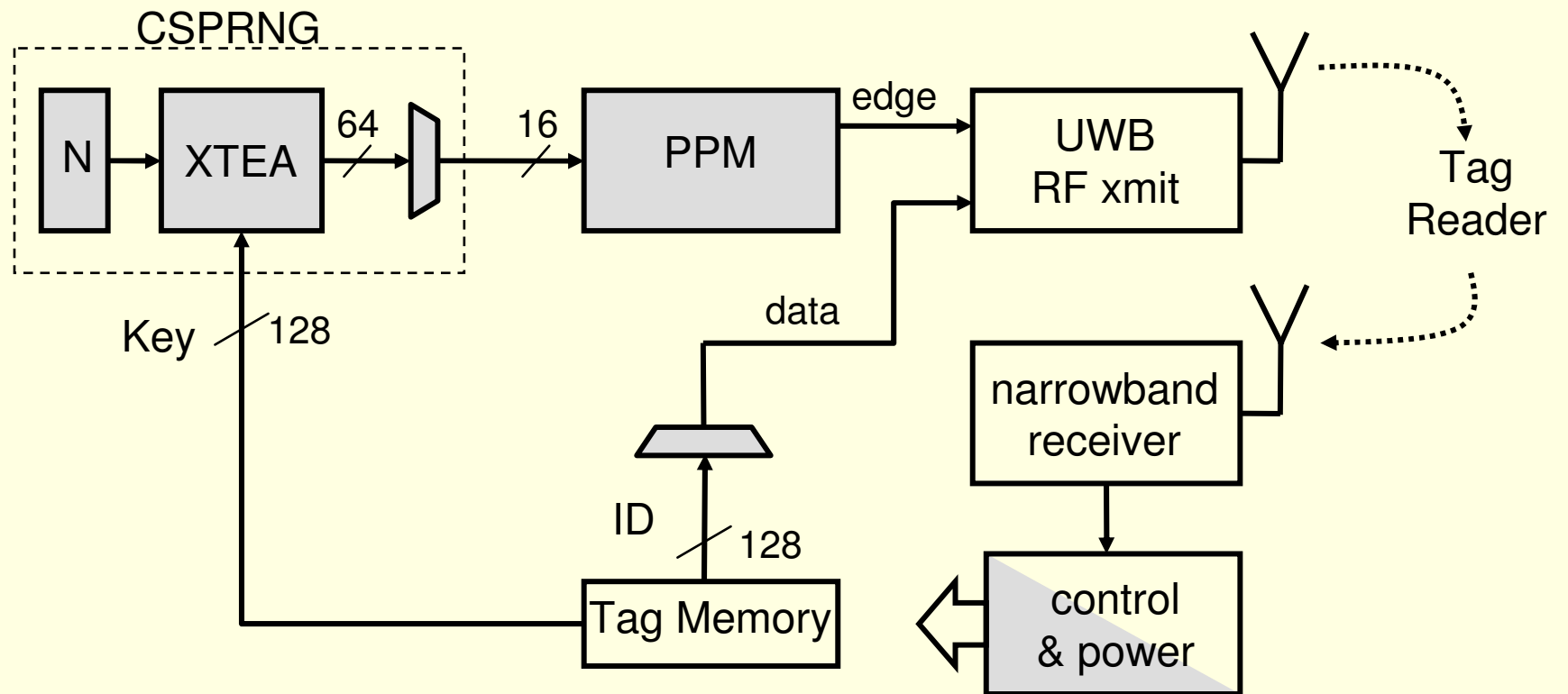


# TH-PPM

---

- CSPRNG determines time-hopping code
- Need to sample all possible time slots if without modulation code
- To eavesdrop:
  - **100 G samples / second**
  - **168 M samples / 8 ms**

# RFID Tag Architecture

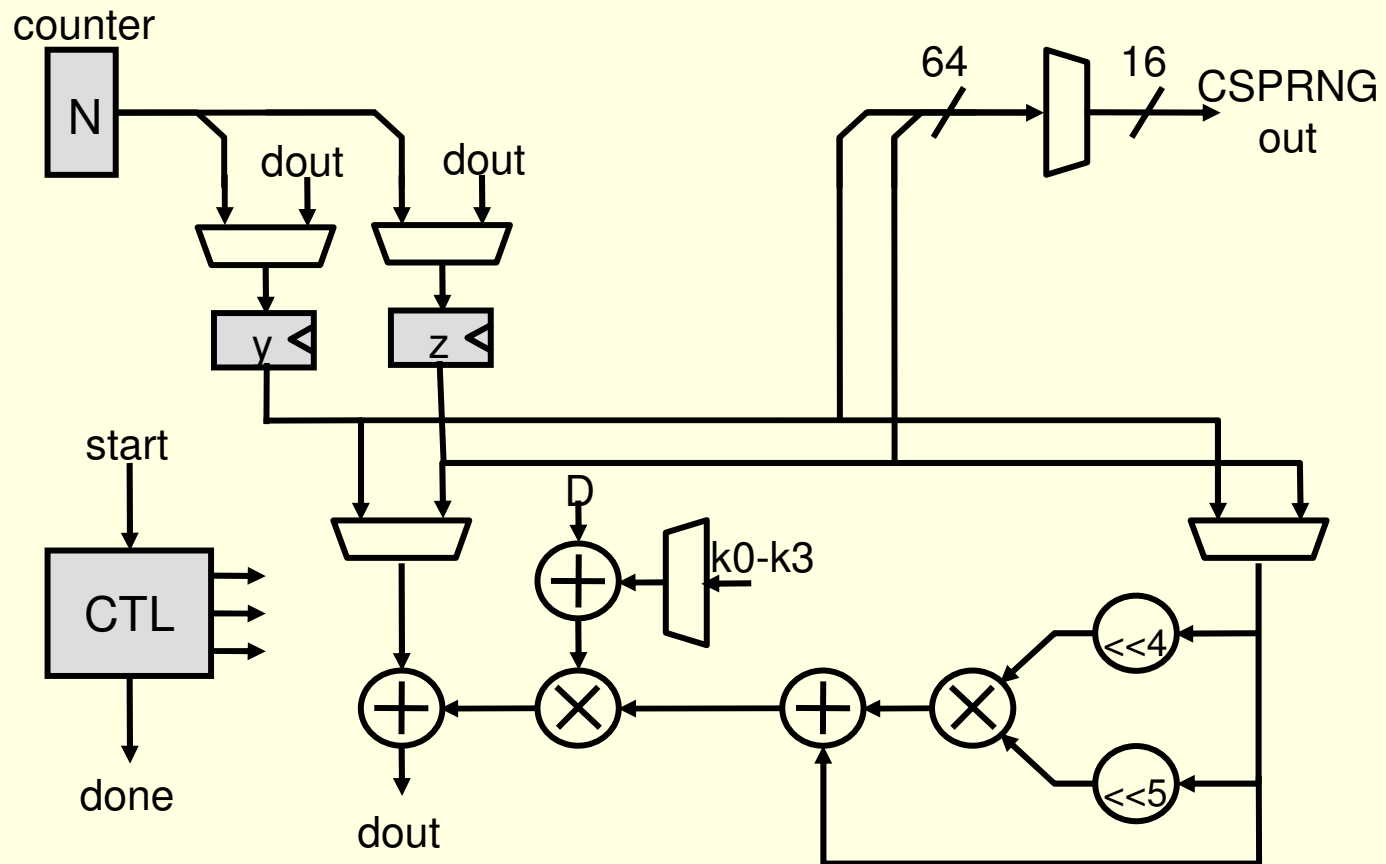


# CSPRNG

---

- Block Cipher running Output-Feedback Mode
- No need for strong encryption primitive such as AES.
- XTEA is chosen for its low area cost and low cycle overhead
  - ~3000 gates with counter registers
  - Only need 64 cycles
  - One round determines four UWB pulse positions

# CSPRNG

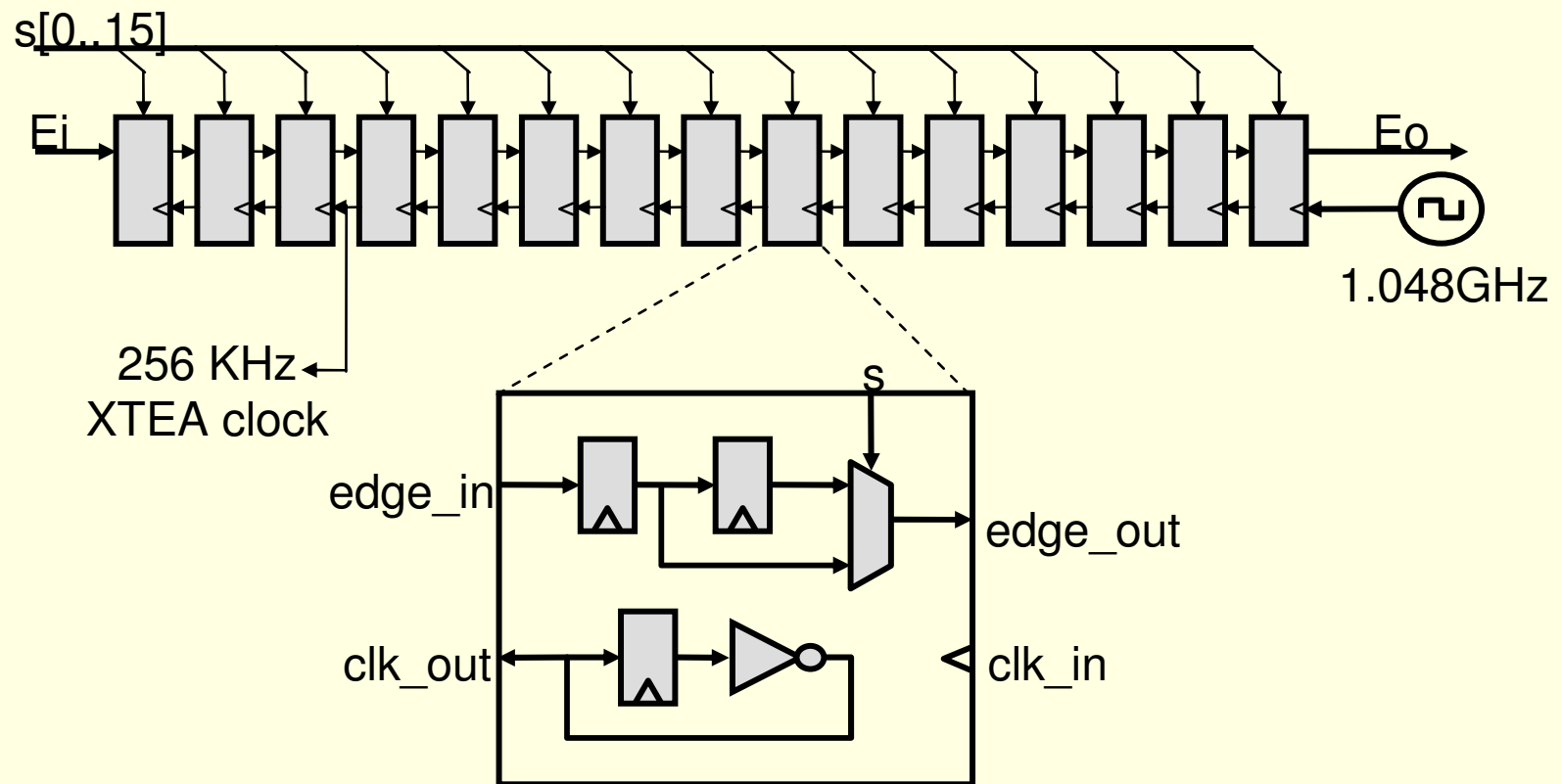


# Pulse Position Modulator

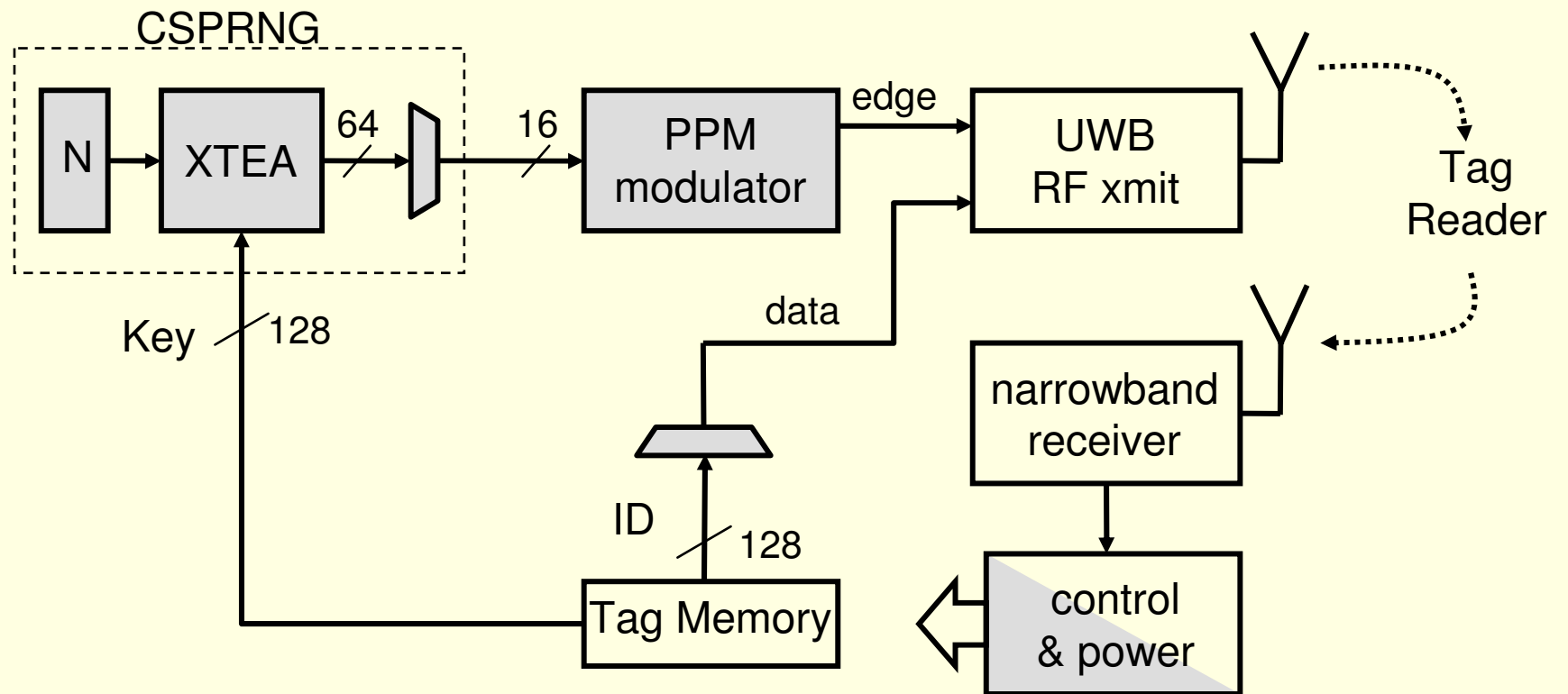
---

- Communicate location of pulses to UWB front-end
- Simple Counter implementation infeasible: whole counter running at 1GHz consumes too much power
- Delay-Chained based implementation used:
  - Most power is consumed at high-frequency clock divider logic.

# Pulse Position Modulator



# RFID Tag Architecture



# Implementation Complexity

	Power*		Gate Count
	Absolute (uW)	Relative	
CSPRNG	14.8	2.10%	3264
Delay Chain	662.0	92.20%	382
Control	41.2	5.70%	990
<b>Overall:</b>	<b>718.0</b>	<b>100.00%</b>	<b>4636</b>

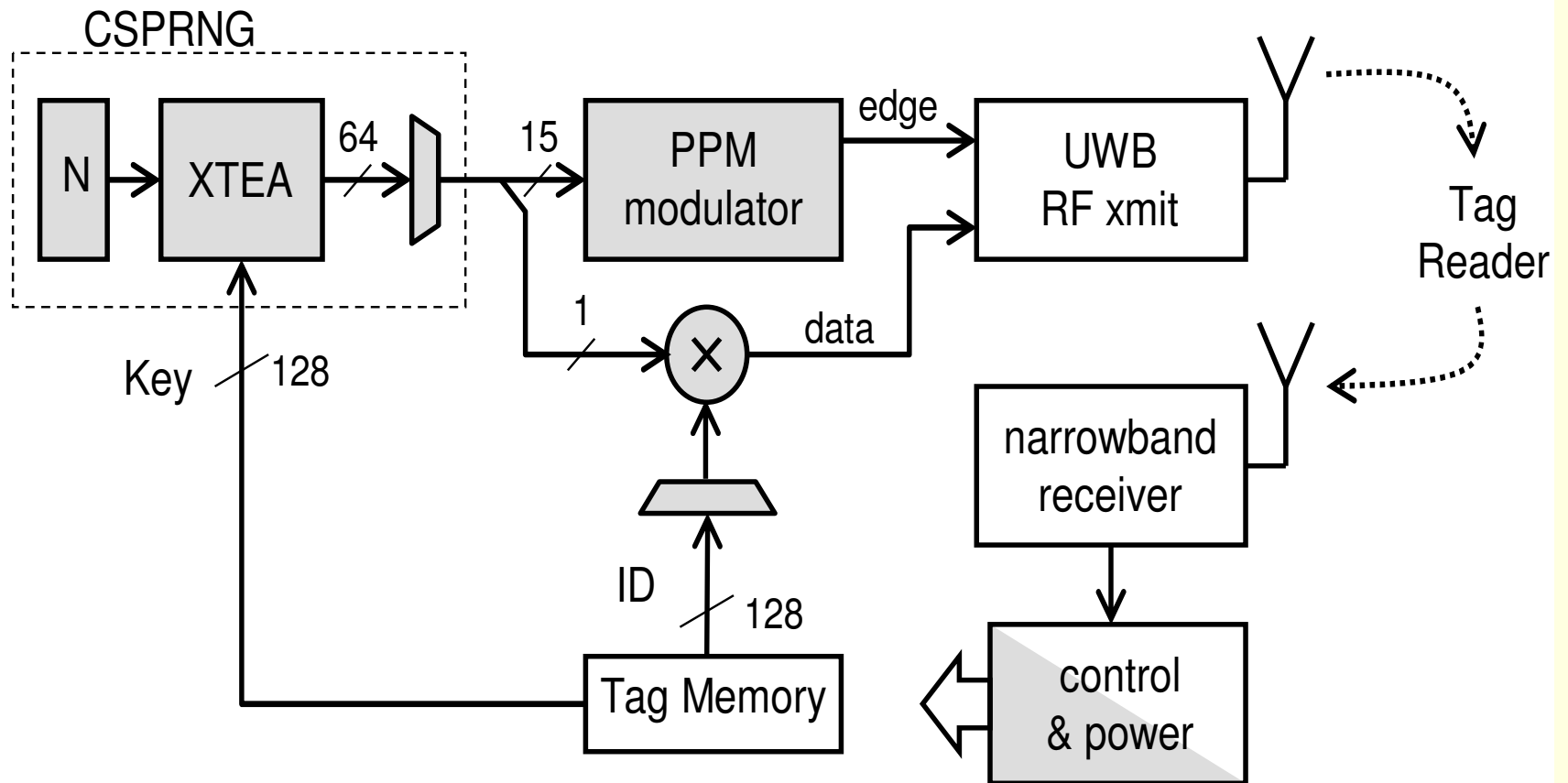
\*TSMC 0.18um CMOS Vdd = 1.8v

# Risk Analysis

---

- Active Attacks
  - Interference / Jamming
- Passive Attacks
  - Eavesdropping

# System Architecture



# Conclusion

---

- Focus on physical layer security
- Results show that the system is technically feasible
- Currently working on:
  - Key distribution
  - UWB front-end
  - Clock generation
  - Investigating multi-access properties of system