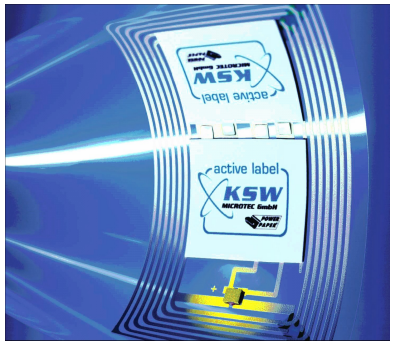
Cryptography for Low Power Devices

Challenge

Providing lightweight cryptographic services that can perform on ultra-low power devices

- Wireless Sensor Nodes (WSN)
  - Medical Monitoring
  - Industrial Monitoring
- Radio Frequency Identification (RFID)
  - Inventory Control
  - Speed-Pass, Car Lock

Source: JHLabs / Dust Inc., ISSS Project, Australia



Source: KSW-microtech Dresden Germany, Smallbiztechnology.com

Low Power Cryptography

Secret-Key Cryptography

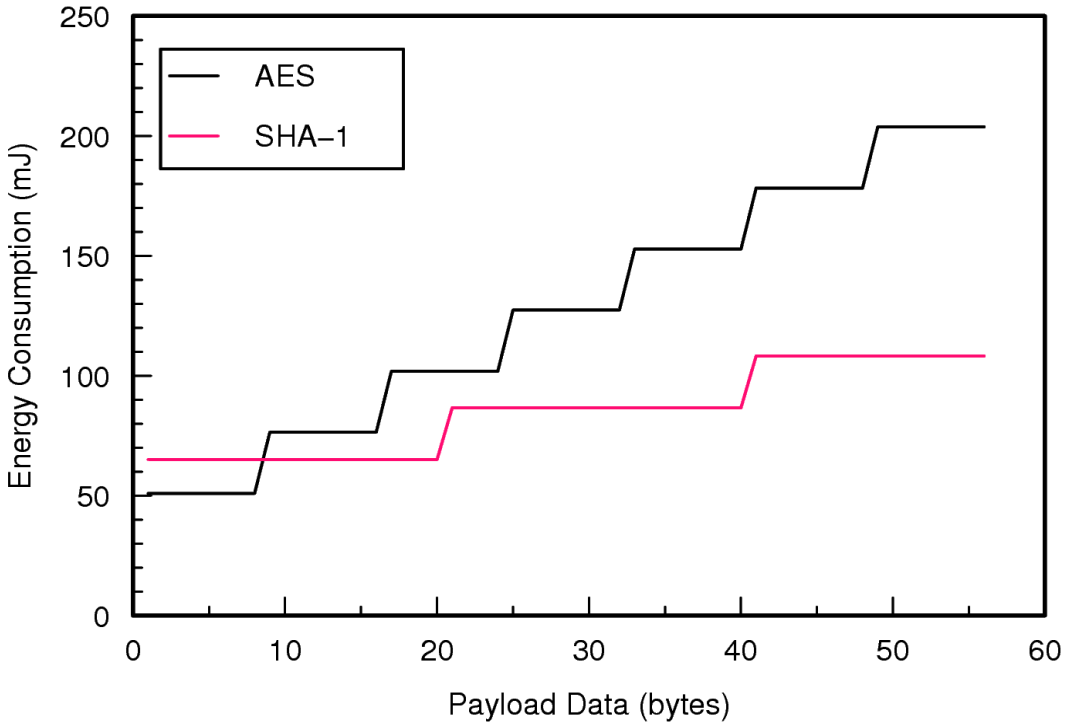
- AES
- TEA
- Present
- Camellia
- Hash Functions
  - SHA-1
  - UMAC

Public-Key Cryptography

- Rabin's Scheme
- NTRU
- ECC
- Identity Based
- Pairing Based

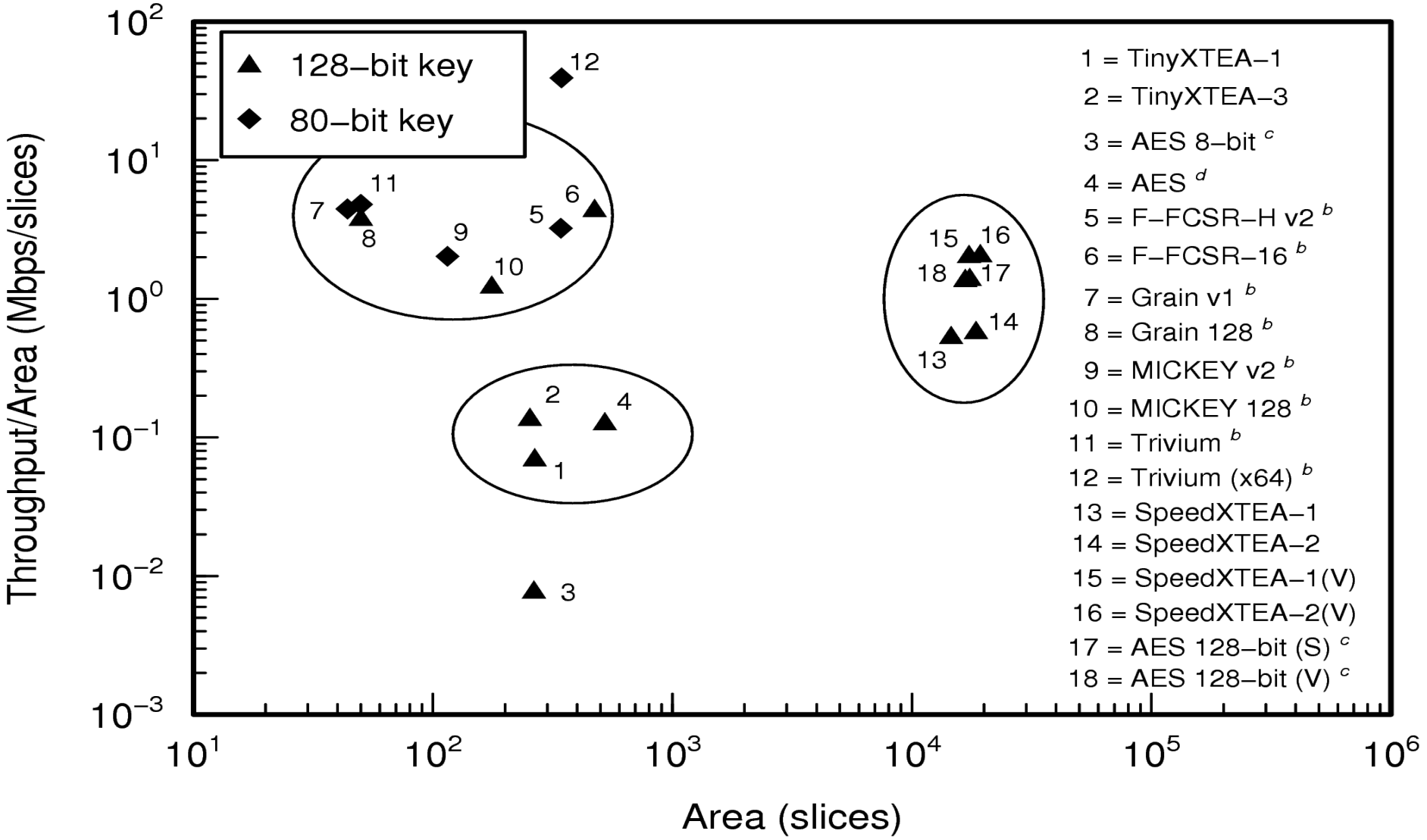
Secret-Key Cryptography

- AES
  - Based on Feldhofer but 47% fewer clock cycles
- SHA-1
- Energy Results
  - Based on TinySec protocol



	MAC		Encryption		Enc & MAC	
	AES	SHA-1	AES	SHA-1	AES	SHA-1
Energy (nJ)	76.42	43.32	50.95	43.32	127.36	86.64
Power (μW)	23.85	26.74	23.85	26.74	23.85	26.74
Time (ms)	3.20	1.62	2.14	1.62	5.34	3.24

Lightweight Ciphers on FPGA



Universal Hash Function

- NH as proposed by Black et al. for UMAC

$$NH_K(M) = \left[\sum_{i=1}^{n/2} \left((m_{2i-1} + k_{2i-1}) \bmod 2^w \right) \cdot \left((m_{2i} + k_{2i}) \bmod 2^w \right) \right] \bmod 2^{2w}$$

- Algorithm Evolution lead to low power optimized

$$NH_K(M) = \left[\sum_{i=1}^{n/2} \left((m_{2i-1} + k_{2i-1}) \bmod 2^w \right) \cdot \left((m_{2i} + k_{2i}) \bmod 2^w \right) \right] \bmod 2^{2w}$$

- Provably secure
- 1/11th of the power consumption

Design	P_{dyn}	P_{Leak}	P	E
NH	5.47 µW	28.1 µW	33.6 µW	4.30 nJ
WH-64	2.26 µW	9.36 µW	11.6 µW	1.49 nJ
WH-32	1.09 µW	4.81 µW	5.9 µW	1.51 nJ
WH-16	0.63 µW	2.32 µW	**2.95 µW**	1.51 nJ

Power and Energy Consumption at 500 kHz

Universal Hash Functions can be used to build unconditionally secure MAC

Public-Key Cryptography

Encryption / Decryption

	Rabin	NtruEncrypt	NtruEncrypt parallel	ECMV
Plain Text Length	< 512 bits	< 265 bits	< 265 bits	< 200 bits
Ciphertext	512 bits	1,169 bits	1,169 bits	400 bits
Packets (30 bytes)	3	5	5	2
		Encryption		
Time	2.88 ms	58.45 ms	0.87 ms	817.7 ms
Avg. Power	148.18 µW	19.13 µW	118.7 µW	394.4 µW
Energy	426.76 nJ	1,118.15 nJ	102.79 nJ	322.5 µJ
		Decryption		
Time	1.089s	116.9 ms	1.732 ms	411.54 ms
Avg. Power	191.5 µW	58.73 µW	158.3 µW	394.4 µW
Energy	208.61 µJ	6,865.54 nJ	274.18 nJ	162.31 µJ

Public-Key Cryptography

Sign and Verify

	Rabin	NtruSign	NtruSign parallel	ECDSA
Signature Length	512 bits	1,169 bits	1,169 bits	200 bits
Packets (30 bytes)	3	5	5	1
		Sign		
Time	1.089s	233.8 ms	3.464 ms	410.45 ms
Avg. Power	191.5 µW	58.73 µW	158.3 µW	394.4 µW
Energy	208.61 µJ	13.73 nJ	548.35 nJ	161.88 µJ
		Verify		
Time	2.88 ms	58.45 ms	0.87 ms	822.5 ms
Avg. Power	148.18 µW	19.13 µW	118.7 µW	394.4 µW
Energy	426.76 nJ	1,118.15 nJ	102.79 nJ	324.39 µJ

New Challenges for Low Power

- Cryptographic Protocols

  Power / Energy used for Computation

  versus

  Power / Energy used for Transmission

- Side Channel Analysis

  Resistance to Attacks

  versus

  Power and Energy Cost