# Implementation of Three LWC Schemes in the WiFi 4-Way Handshake with Software Defined Radio

Yunjie Yi, Guang Gong, Kalikinkar Mandal
{yunjie.yi,ggong,kmandal}@uwaterloo.ca

Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, ON, N2L 3G1, CANADA

November 4 - 6, 2019

Third Lightweight Cryptography Workshop 2019 at NIST

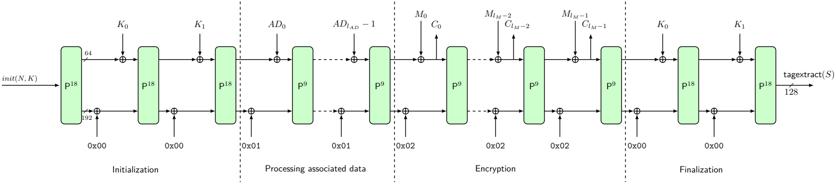
# Outline

1. Background
   - SPIX, ACE and WAGE algorithms
   - IEEE 802.1a PHY 4-way handshake and data protection
   - Software defined radio
2. Implementation of Three LWC Schemes
   - KDF and MIC generation
   - Implementation on microcontrollers
3. Performance Results
   - KDF and MIC for 4-way handshake
   - SPIX, ACE and WAGE for data protection

# SPIX: An authenticated encryption algorithm

## Design[1]

- Adopts the monkey duplex mode of operation
- Underlying permutation: sLiSCP-light-256[2]
- 128-bit security with straight out parameters:
  key size = tag size = nonce size = security level
- Data limit: $2^{63}$ bytes before re-keying is done




SPIX AE algorithm

1 Altawy, R., Gong, G., He, M., Mandal, K., and Rohit, R. SPIX: An authenticated cipher. NIST LWC round 2 candidate. (2019)

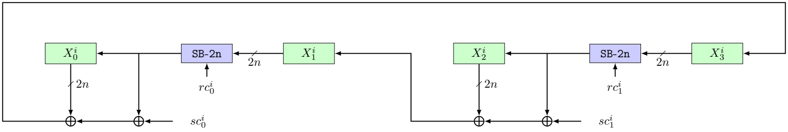
2 Altawy, R., Rohit, R., He, M., Mandal, K., Yang, G., and Gong, G. sLiSCP-light: Towards hardware optimized sponge-specific cryptographic permutations. ACM Trans. Embedded Computing Systems. (2018)

# SPIX (Cont.)

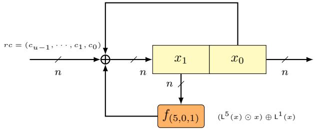
sLiSCP-light permutation round function

State: $X^i = (X_0^i, X_1^i, X_2^i, X_3^i)$ with size 256 bits

Simeck box: $\texttt{SB-}2n$ where $n = 32$




sLiSCP-light permutation step function

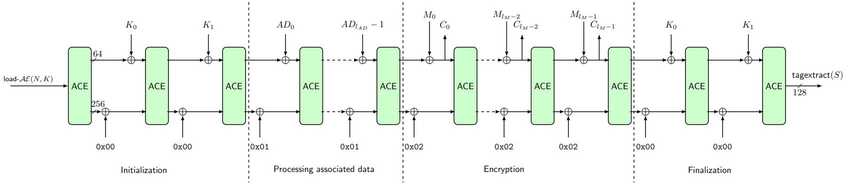



Simeck (SB-2n)

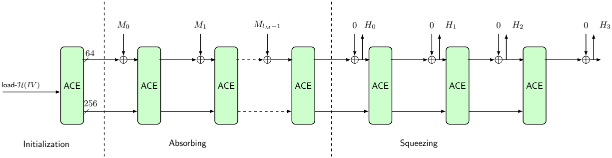
# ACE: An AE and hash algorithm

## Design goals

- Both AE and Hash functionalities with a single hardware footprint
- 128-bit security level with good security margins
- Balance among hardware cost and software efficiency

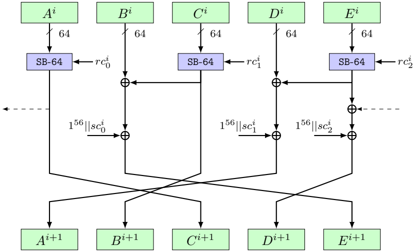



(a) ACE Authenticated encryption algorithm




(b) ACE Hash algorithm

# ACE Permutation




ACE permutation step function

## Parameters[1]

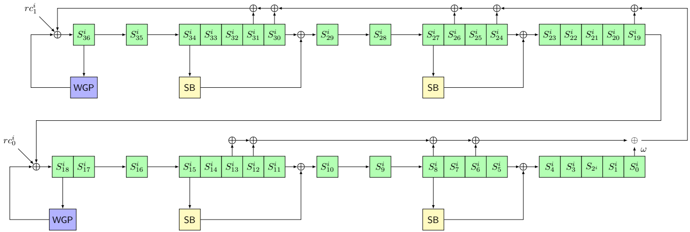
- State size: 320 bits
- Nonlinear layer: 3 SB-64 (Simeck) boxes
- Linear layer ($\sigma$): (3,2,0,4,1)
- # rounds($u$)/steps($s$): 8/16
- Rate positions: 4 bytes of A$[7, \cdots, 4]$ and C$[7, \cdots, 4]$
- 8-bit round and step constants $rc_j^i$ and $sc_j^i$

[1] Aagaard, M., AlTawy, R., Gong, G., Mandal, K., and Rohit, R. ACE: An authenticated encryption and hash algorithm. NIST LWC round 2 candidate. (2019)

# WAGE: An authenticated encryption algorithm

## Design[1]

- Underlying permutation: WAGE (over extension field $\mathbb{F}_{2^7}$) of width 259 bits
- Round function of WAGE is constructed by tweaking the initialization phase of the WG stream cipher
- Mode of operation: Similar to ACE
- \# rounds: 111
- 128-bit security, low hardware cost
- Data limit: $2^{64}$ bytes




1 Aagaard, M., AlTawy, R., Gong, G., Mandal, K., Rohit, R and Zidaric, N. WAGE: An authenticated cipher. NIST LWC round 2 candidate. (2019)

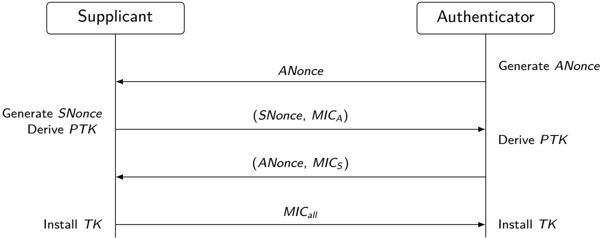
# IEEE 802.1X 4-way handshake and data protection

## 4-way handshake and data protection

- 4-way handshake: Conducts mutual entity authentication and generation of session keys
- Data protection: After 4-way handshake, it executes a data protection protocol, either CCMP or GCMP

  CCMP: AES in counter mode + CBC MAC

  GCMP: AES in counter mode + polynomial hash for MAC



# IEEE 802.1X (Cont.)

**Computing keys in the 4-way handshake protocol**

- Pairwise transit key (PTK) is generated as

$$PTK = KDF(PMK, ANonce||SNonce||\text{AP MAC adr}||\text{STA MAC adr})$$

$$PTK = KCK||KEK||TK$$

  - $KCK$ is used to generate a MIC
  - $KEK$ is used for encrypting the group key
  - $TK$ is used for protecting traffic data

- Message integrity codes (MICs) are generated as

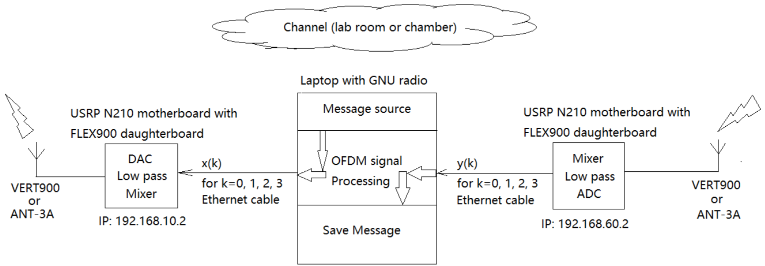
$$MIC_A = MIC(KCK, ANonce, r)$$
$$MIC_S = MIC(KCK, SNonce, r)$$
$$MIC_{all} = MIC(KCK, D, r+1)$$

where $r$ is a replay counter number, and $D$ carries the cipher suite.

# Software defined radio (SDR)

## SDR setup

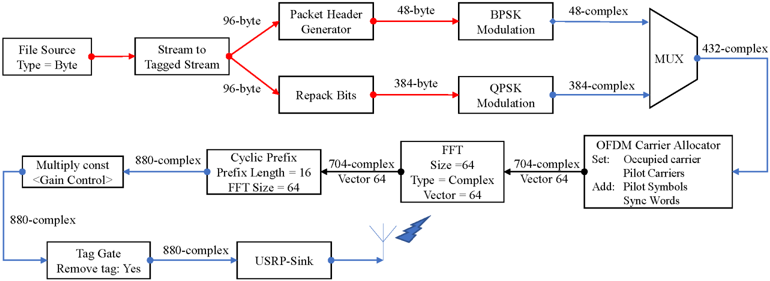
- SDR has two main parts: Universal Software Radio Peripheral (USRP) and GNU radio
- USRP is a hardware consisting of ADC, DAC, low pass filer and mixer
- GNU radio is a digital signal processing (DSP) software on a Linux OS



# OFDM sender in SDR

## OFDM sender

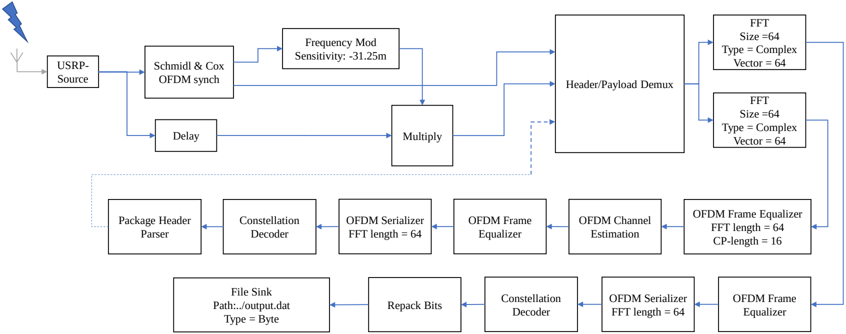
- The digital processing part before the USRP sender are done on PC in real time
- The OFDM sender includes package header generator, modulation, carrier allocator, cyclic prefix and so on



# OFDM receiver in SDR

## OFDM receiver

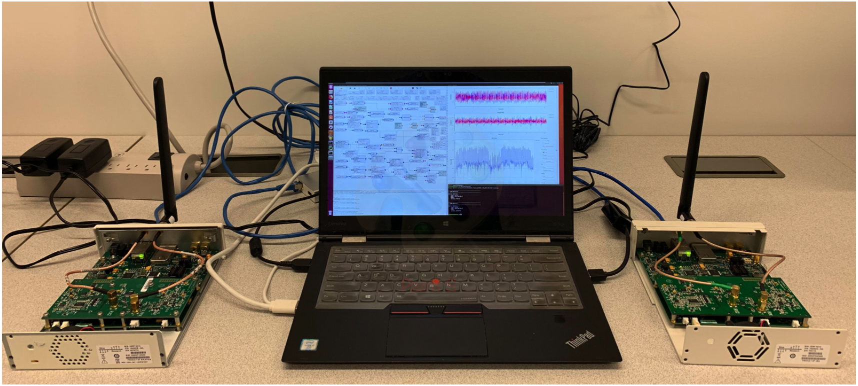
- USRP receiver received sampled data in complex domain
- The receiver contains synchronization module, header and payload demux, OFDM demodulation and so on



# Our Contribution

# Implementation of IEEE802.11a PHY in SDR

- One USRP is configured as a supplicant and another is an authenticator
- Two USRPs communicate wirelessly

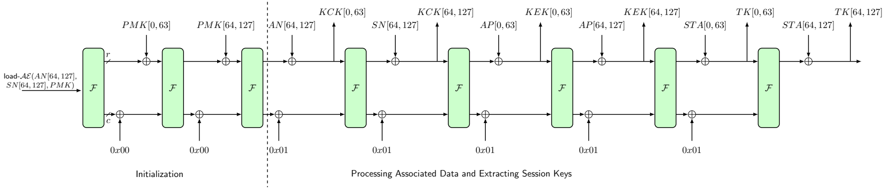


# Implementation of $KDF$ and $MIC$

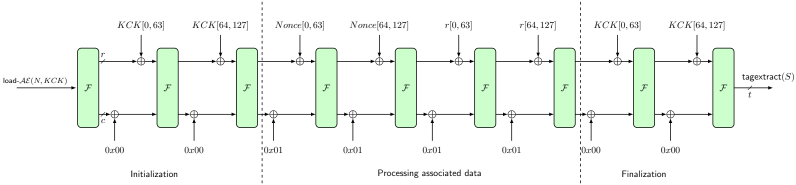
## Implementation - $KDF$ and $MIC$

- Sponge structure is used for KDF and generation of $MIC$
- SPIX, ACE and WAGE follow the same framework

### Key derivation function construction




### Message integrity code generation



# Microcontroller implementations: SPIX, ACE and WAGE

## Microcontroller platform specifications[3]

- SPIX, ACE and WAGE are implemented in assembly language
- SPIX: 8-bit, 16-bit and 32-bit microcontrollers Atmega128, MSP430 and Cortex-M3
- ACE: 16-bit and 32-bit microcontrollers MSP430 and Cortex-M3
- WAGE: 8-bit, 16-bit and 32-bit microcontrollers Atmega128, MSP430 and Cortex-M3
- Clock frequency: 16 MHz for all platforms

| Microcontrollers | Flash memory size [kB] | RAM [kB] | Number of general-purpose register |
|---|---|---|---|
| ATmega128(SPIX, WAGE) | 128 | 4.448 | 32(R0 - R31) |
| MSP430F2013(ACE, SPIX) | 2.304 | 0.128 | 12 (R4 - R15) |
| MSP430F2370(WAGE) | 33.024 | 2.048 | 12 (R4 - R15) |
| LM3S9D96(ACE, SPIX, WAGE) | 524.288 | 131.072 | 13 (R0 - R12) |

[3] Cortex-M3: Cortex-m3lm3s9d96, MSP430: MSP430f2013

# Implementation Details

- For SPIX, the state is stored in the registers
- For ACE and WAGE, the state is stored in memory
- Instead of loading everything into registers, the WAGE state is continuously stored in random access memory (RAM)
  - Initial memory location and the current round is recorded
  - After the permutation evaluation, copy the final state to the initial state location in RAM
  - Continue the next WAGE permutation evaluation

# Performance of 4-way handshake authentication

## Authentication time

- Auth-Time includes the 4-way transmission time + computation times of $KDF$ and $MIC$ functions

$$T_{auth} = T_{4-way-tx} + 2 * T_{KDF} + 3 * T_{MIC}.$$

- $KDF$ computation is equivalent to AE($l_{AD} = 0$, $l_M = 6$), no tag
- $MIC$ computation is equivalent to AE($l_{AD} = 4$, $l_M = 0$), with tag

| Cryptographic $\mathcal{F}$ | Platform | Function | Memory usage [Bytes] | | Setup [Cycles] | Throughput [Kbps] | Gen-time [ms] | 4-way-Tx-time [ms] | Auth-Time [ms] |
|---|---|---|---|---|---|---|---|---|---|
| | | | SRAM | Flash | | | | | |
| SPIX | 8-bits ATmega128 | KDF | 175 | 1586 | 705314 | 23.23 | 44.08 | 700 | 956.40 |
| | | MIC | 175 | 1634 | 897225 | 18.26 | 56.08 | | |
| | 16-bits MSP430F2013 | KDF | 50 | 1562 | 286679 | 57.15 | 17.92 | 690 | 794.09 |
| | | MIC | 50 | 1580 | 363991 | 45.01 | 22.75 | | |
| | 32-bits LM3S9D96 | KDF | 408 | 1230 | 59140 | 277.04 | 3.70 | 700 | 721.50 |
| | | MIC | 408 | 1326 | 75132 | 218.07 | 4.70 | | |
| ACE | 16-bits MSP430F2013 | KDF | 330 | 1720 | 550752 | 29.75 | 34.42 | 710 | 895.03 |
| | | MIC | 330 | 1738 | 619701 | 26.44 | 38.73 | | |
| | 32-bits LM3S9D96 | KDF | 599 | 1826 | 102762 | 159.44 | 6.42 | 730 | 764.50 |
| | | MIC | 599 | 1790 | 115561 | 141.78 | 7.22 | | |
| WAGE | 8-bits ATmega128 | KDF | 808 | 4448 | 139478 | 117.47 | 8.72 | 710 | 756.78 |
| | | MIC | 808 | 4516 | 156491 | 104.70 | 9.78 | | |
| | 16-bits MSP430F2013 | KDF | 46 | 4518 | 166993 | 98.11 | 10.44 | 720 | 776.01 |
| | | MIC | 46 | 4536 | 187340 | 87.46 | 11.71 | | |
| | 32-bits LM3S9D96 | KDF | 3084 | 6278 | 107071 | 153.02 | 6.69 | 690 | 725.91 |
| | | MIC | 3084 | 6382 | 120190 | 136.32 | 7.51 | | |

SPIX implementation is faster due to storing state into registers

# SPIX for IEEE 802.11i data protection protocol

- 32-bit Cortex-M3 gives the highest throughput and lowest memory usage
- Total time for no AD and 128 bytes message: 1058 ms
- Total time for 16 byte AD and 128 bytes message: 1079 ms

| Cryptographic | Platform | Memory usage [Bytes] | | Setup [Cycles] | Throughput [Kbps] | Gen-time [ms] | Tx-time [ms] |
|---|---|---|---|---|---|---|---|
| | | SRAM | Flash | | | | |
| SPIX Perm-18 | 8-bits ATmega128 | 161 | 1262 | 128377 | 31.91 | 8.02 | N/A |
| | 16-bits MSP430F2013 | 24 | 1409 | 52294 | 78.33 | 3.27 | |
| | 32-bits LM3S9D96 | 352 | 946 | 10900 | 375.78 | 0.68 | |
| SPIX-AE ($l_{AD} = 0$, $l_M = 16$) | 8-bits ATmega128 | 175 | 1550 | 1667042 | 9.83 | 104.19 | 1060 |
| | 16-bits MSP430F2013 | 50 | 1845 | 677818 | 24.17 | 42.36 | 1080 |
| | 32-bits LM3S9D96 | 408 | 1210 | 139569 | 117.39 | 8.72 | 1050 |
| SPIX-AE ($l_{AD} = 2$, $l_M = 16$) | 8-bits ATmega128 | 175 | 1644 | 1795322 | 9.13 | 112.21 | 1080 |
| | 16-bits MSP430F2013 | 50 | 1891 | 730340 | 22.43 | 45.65 | 1050 |
| | 32-bits LM3S9D96 | 424 | 1326 | 150313 | 109.00 | 9.39 | 1070 |

# ACE for IEEE 802.11i data protection protocol

- 32-bit Cortex-M3 gives the best result
- Total time for no AD and 128 bytes message: 1087 ms
- Total time for 16 byte AD and 128 bytes message: 1098 ms

| Cryptographic | Platform | Memory usage [Bytes] | | Setup [Cycles] | Throughput [Kbps] | Gen-time [ms] | Tx-time [ms] |
|---|---|---|---|---|---|---|---|
| | | SRAM | Flash | | | | |
| ACE Perm | 16-bits MSP430F2013 | 304 | 1456 | 69440 | 73.73 | 4.34 | N/A |
| | 32-bits LM3S9D96 | 523 | 1598 | 13003 | 393.76 | 0.81 | |
| ACE-AE ($l_{AD} = 0$, $l_M = 16$) | 16-bits MSP430F2013 | 330 | 1740 | 1445059 | 11.34 | 90.32 | 1060 |
| | 32-bits LM3S9D96 | 559 | 1790 | 269341 | 60.83 | 16.83 | 107 |
| ACE-AE ($l_{AD} = 2$, $l_M = 16$) | 16-bits MSP430F2013 | 330 | 1786 | 1582892 | 10.35 | 98.93 | 1080 |
| | 32-bits LM3S9D96 | 559 | 1858 | 294988 | 55.54 | 18.44 | 1080 |
| ACE-Hash ($l_M = 2$, $j$ =4) | 16-bits MSP430F2013 | 330 | 1682 | 413056 | 4.96 | 25.82 | N/A |
| | 32-bits LM3S9D96 | 559 | 1822 | 77114 | 26.56 | 4.82 | |
| ACE-Hash ($l_M = 16$, $j$ =4) | 16-bits MSP430F2013 | 330 | 1684 | 1375672 | 11.91 | 85.98 | |
| | 32-bits LM3S9D96 | 559 | 1822 | 256524 | 63.87 | 16.03 | |

# WAGE for IEEE 802.11i data protection protocol

- Cortex-M3 gives the highest throughput with highest memory usage
- MSP430 gives the slightly lower throughput but much lower memory usage
- Total time for no AD and 128 bytes message: 1077 ms
- Total time for 16 byte AD and 128 bytes message: 1079 ms

| Cryptographic | Platform | Memory usage [Bytes] | | Setup [Cycles] | Throughput [Kbps] | Gen-time [ms] | Tx-time [ms] |
|---|---|---|---|---|---|---|---|
| | | SRAM | Flash | | | | |
| WAGE Perm | 8-bits ATmega128 | 802 | 4132 | 19011 | 217.98 | 1.19 | N/A |
| | 16-bits MSP430F2370 | 4 | 5031 | 23524 | 176.16 | 1.47 | |
| | 32-bits LM3S9D96 | 3076 | 5902 | 14450 | 286.78 | 0.9 | |
| WAGE-AE ($l_{AD} = 0$, $l_M = 16$) | 8-bits ATmega128 | 808 | 4416 | 362888 | 45.15 | 22.68 | 1080 |
| | 16-bits MSP430F2370 | 46 | 5289 | 433105 | 37.83 | 27.07 | 1090 |
| | 32-bits LM3S9D96 | 3084 | 6230 | 278848 | 58.76 | 17.43 | 1060 |
| WAGE-AE ($l_{AD} = 2$, $l_M = 16$) | 8-bits ATmega128 | 808 | 4502 | 397260 | 41.24 | 24.83 | 1050 |
| | 16-bits MSP430F2370 | 46 | 5339 | 474067 | 34.56 | 29.63 | 1060 |
| | 32-bits LM3S9D96 | 3084 | 6354 | 305284 | 53.67 | 19.08 | 1060 |

# Conclusions

- Implemented the IEEE 802.11a physical layer OFDM transmission systems by software defined radio to simulate the 4-way handshake modulation and communication

- Implemented the IEEE 802.1x 4-way handshake mutual authentication and key establishment protocol using SPIX, ACE, and WAGE, on three different microcontrollers

- Throughput of WAGE is higher than that of AES-128 written in C[1] on the same 8-bit platform.

- Execution time for the cryptographic operations is the dominating factor in the 4-way handshake.
  - USRP tx rate: 16.82 Kbps
  - WiFi system's tx rate: 50 - 320 Mbps
  - Scaling tx to WiFi: $\frac{0.7\times 16.82}{50000} = 0.235$ ms

[1] G. Meiser, T. Eisenbarth, K. Lemke-Rust, and C. Paar. Efficient implementation of estream ciphers on 8-bit avr microcontrollers. In 2008 International Symposium on Industrial Embedded Systems, pages 58 - 66, June 2008

Thank you!