Quantum Key-Recovery on Full AEZ

Xavier Bonnetain

Sorbonne Université, Inria, France

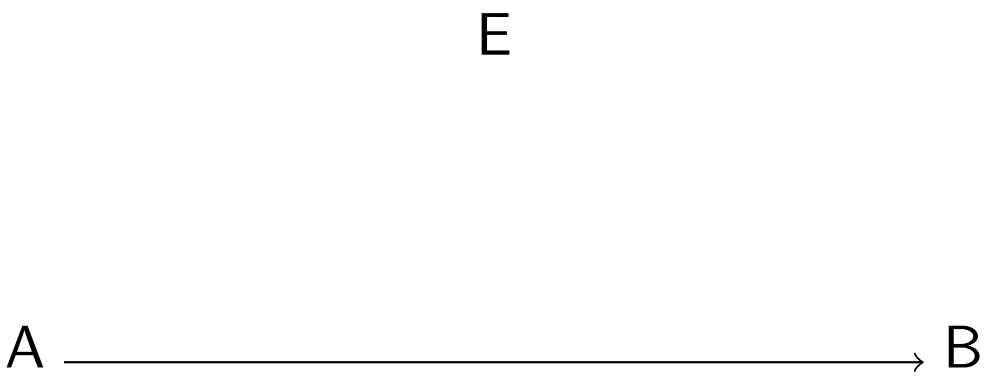
Friday 19th January, 2018

Reference

Xavier Bonnetain.
Quantum key-recovery on full AEZ.
In *SAC 2017*, pages 394–406, 2017.

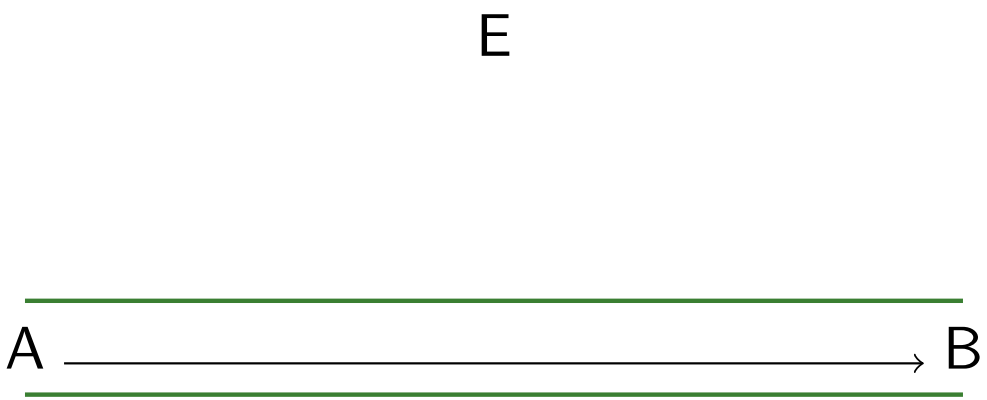
Outline

Cryptography



Properties

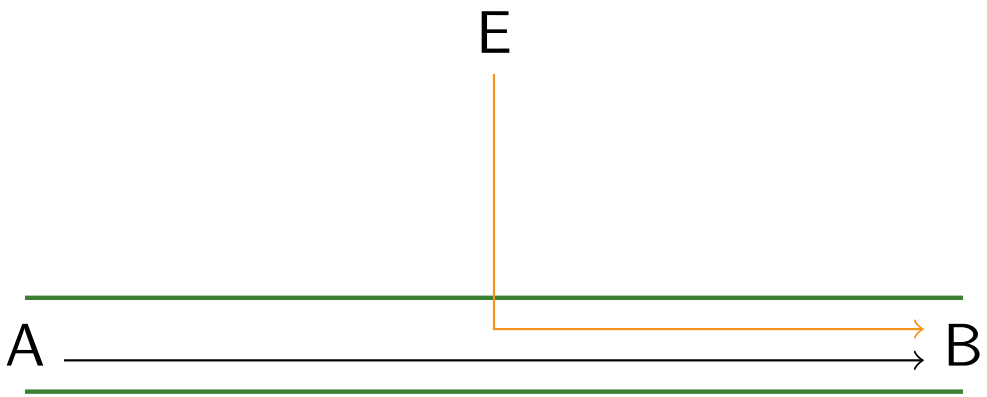
Cryptography



Properties

- Confidentiality

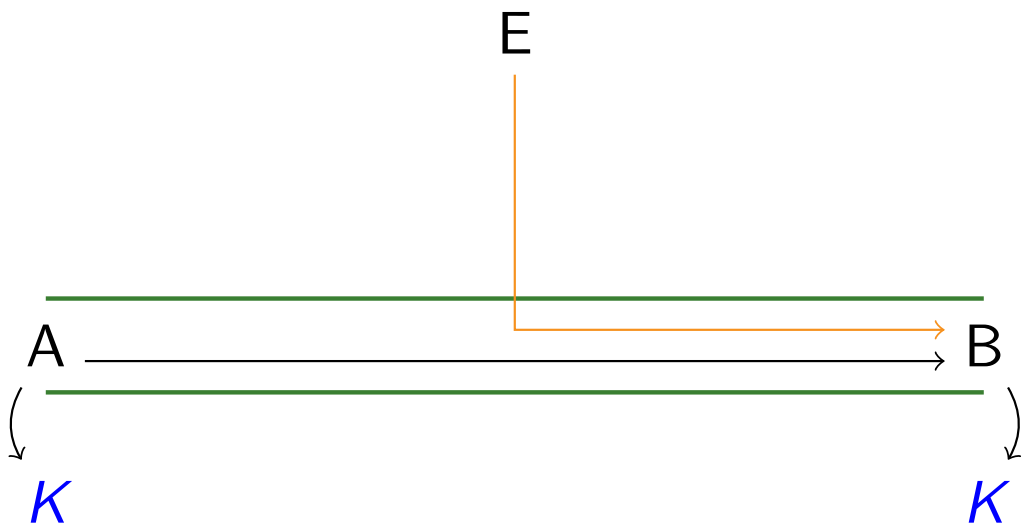
Cryptography



Properties

- Confidentiality
- Integrity

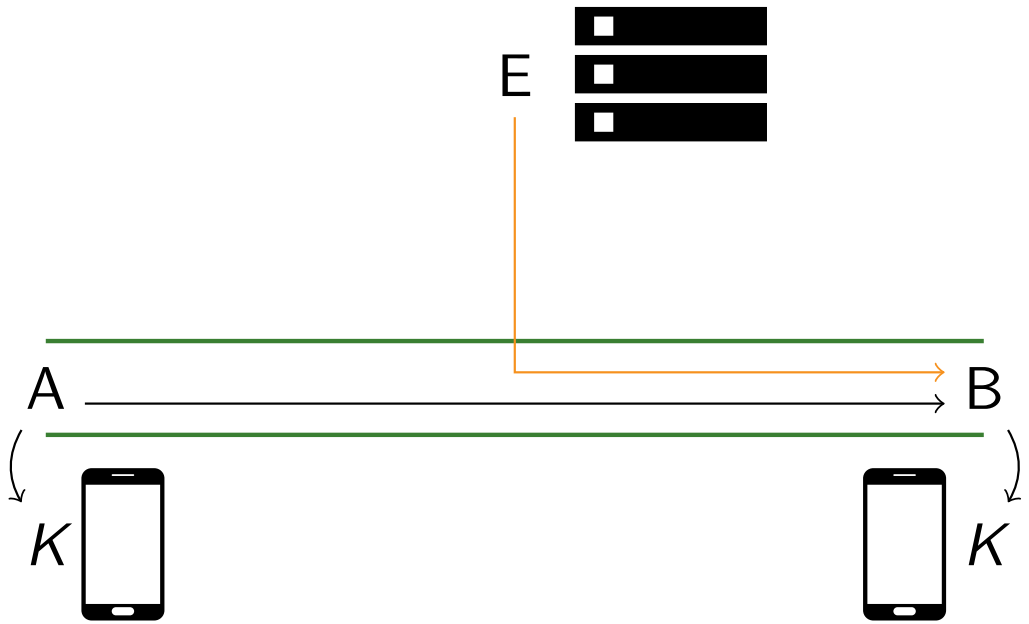
Symmetric Cryptography



Properties

- Confidentiality
- Integrity

Symmetric Cryptography

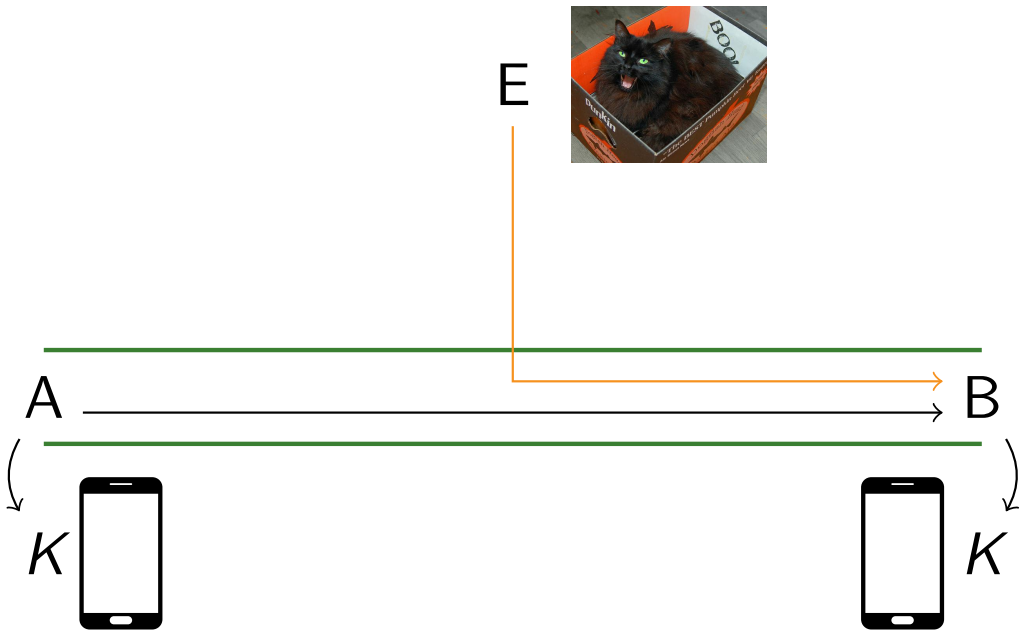


Properties

- Confidentiality
- Integrity

Classical model

Symmetric Cryptography

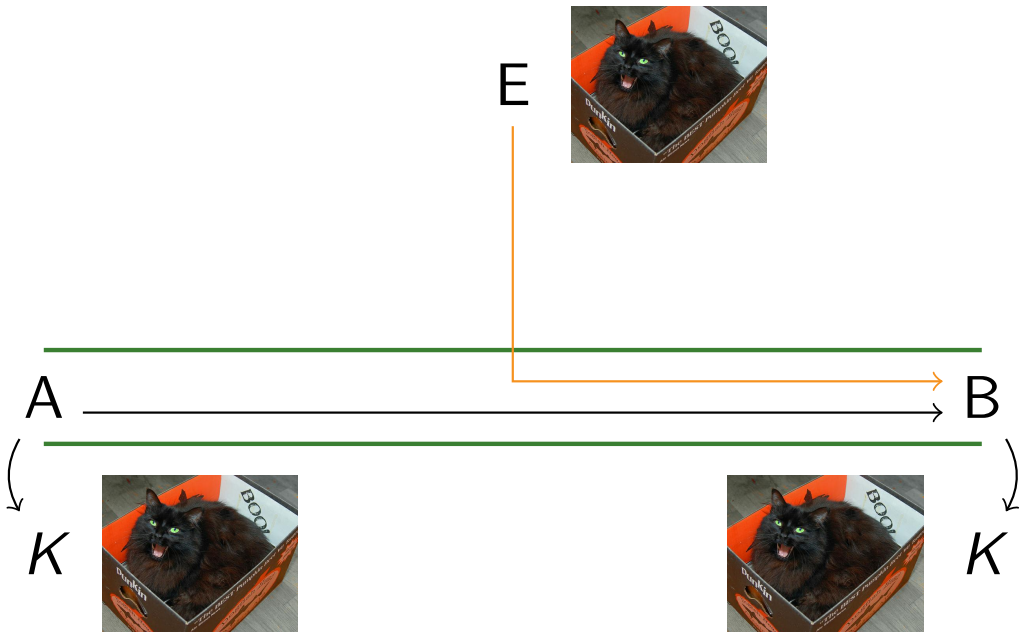


Properties

- Confidentiality
- Integrity

Quantum computation model (Q1)

Symmetric Cryptography



Properties

- Confidentiality
- Integrity

Quantum query model (Q2)

CAESAR competition

- Competition to choose a portfolio of authenticated encryption primitives
- 50+ candidates for the first round
- 15 remain for the third round (including AEZ)

History of AEZ [HKR15]

- AEZv3 : A birthday analysis recovers the key [FLS15]

History of AEZ [HKR15]

- AEZv3 : A birthday analysis recovers the key [FLS15]
- AEZv4 uses Blake2, more complex offsets.

History of AEZ [HKR15]

- AEZv3 : A birthday analysis recovers the key [FLS15]
- AEZv4 uses Blake2, more complex offsets.
- AEZv4 : A birthday analysis recovers the key [CG16]

History of AEZ [HKR15]

- AEZv3 : A birthday analysis recovers the key [FLS15]
- AEZv4 uses Blake2, more complex offsets.
- AEZv4 : A birthday analysis recovers the key [CG16]
- A bug in the offsets allowed simple forgeries [BDDJLMS17]

History of AEZ [HKR15]

- AEZv3 : A birthday analysis recovers the key [FLS15]
- AEZv4 uses Blake2, more complex offsets.
- AEZv4 : A birthday analysis recovers the key [CG16]
- A bug in the offsets allowed simple forgeries [BDDJLMS17]
- AEZv5 uses simpler and safer offsets.

Overview of AEZ

- Fast, AES-based authenticated encryption with associated data,
- Security claimed up to 2^{48} bytes of encryption, 2^{128} time.

AEZ in details

100 **algorithm** Encrypt$(K, N, \boldsymbol{A}, \tau, M)$ // AEZ authenticated encryption
101 $X \leftarrow M \,\|\, 0^\tau$; $(A_1, \ldots, A_a) \leftarrow \boldsymbol{A}$
102 $\boldsymbol{T} \leftarrow ([\tau]_{128}, N, A_1, \ldots, A_a)$
103 **if** $M = \varepsilon$ **then return** AEZ-prf$(K, \boldsymbol{T}, \tau)$
104 **return** Encipher$(K, \boldsymbol{T}, X)$

110 **algorithm** Decrypt$(K, N, \boldsymbol{A}, \tau, C)$ // AEZ authenticated decryption
111 $(A_1, \ldots, A_a) \leftarrow \boldsymbol{A}$; $\boldsymbol{T} \leftarrow ([\tau]_{128}, N, A_1, \ldots, A_a)$
112 **if** $|C| < \tau$ **then return** $\perp$
113 **if** $|C| = \tau$ **then if** $C =$ AEZ-prf$(K, \boldsymbol{T}, \tau)$ **then return** ε **else return** $\perp$ **fi fi**
114 $X \leftarrow$ Decipher$(K, \boldsymbol{T}, C)$
115 $M \,\|\, Z \leftarrow X$ where $|Z| = \tau$
116 **if** $(Z = 0^\tau)$ **then return** M **else return** $\perp$

200 **algorithm** Encipher$(K, \boldsymbol{T}, X)$ // AEZ enciphering
201 **if** $|X| < 256$ **then return** Encipher-AEZ-tiny$(K, \boldsymbol{T}, X)$
202 **if** $|X| \geq 256$ **then return** Encipher-AEZ-core$(K, \boldsymbol{T}, X)$

210 **algorithm** Encipher-AEZ-tiny$(K, \boldsymbol{T}, M)$ // AEZ-tiny enciphering
211 $\mu \leftarrow |M|$; $n \leftarrow \mu/2$; $\Delta \leftarrow$ AEZ-hash$(K, \boldsymbol{T})$
212 **if** $\mu = 8$ **then** $k \leftarrow 24$ **else if** $\mu = 16$ **then** $k \leftarrow 16$ **else if** $\mu < 128$ **then** $k \leftarrow 10$ **else** $k \leftarrow 8$ **fi**
213 $L \leftarrow M[1\,..\,n]$; $R \leftarrow M[n+1\,..\,\mu]$; **if** $\mu \geq 128$ **then** $i \leftarrow 6$ **else** $i \leftarrow 7$ **fi**
214 **for** $j \leftarrow 0$ **to** $k-1$ **do** $R' \leftarrow L \oplus ((\mathrm{E}_K^{0,i}(\Delta \oplus R10^* \oplus [j]_{128}))[1\,..\,n])$; $L \leftarrow R$; $R \leftarrow R'$ **od**
215 $C \leftarrow R \,\|\, L$; **if** $\mu < 128$ **then** $C \leftarrow C \oplus (\mathrm{E}_K^{0,3}(\Delta \oplus (C0^* \vee 10^*)) \wedge 10^*)$ **fi**
216 **return** C

220 **algorithm** Encipher-AEZ-core$(K, \boldsymbol{T}, M)$ // AEZ-core enciphering
221 $\Delta \leftarrow$ AEZ-hash$(K, \boldsymbol{T})$
222 $M_1 M_1' \cdots M_m M_m'$ M_{uv} $M_{\mathsf{x}} M_{\mathsf{y}} \leftarrow M$ where $|M_1| = \cdots = |M_m'| = |M_{\mathsf{x}}| = |M_{\mathsf{y}}| = 128$ and $|M_{\mathsf{uv}}| < 256$
223 $d \leftarrow |M_{\mathsf{uv}}|$; **if** $d \leq 127$ **then** $M_{\mathsf{u}} \leftarrow M_{\mathsf{uv}}$; $M_{\mathsf{v}} \leftarrow \varepsilon$ **else** $M_{\mathsf{u}} \leftarrow M_{\mathsf{uv}}[1..128]$; $M_{\mathsf{v}} \leftarrow M_{\mathsf{uv}}[129..|M_{\mathsf{uv}}|]$ **fi**
224 **for** $i \leftarrow 1$ **to** m **do** $W_i \leftarrow M_i \oplus \mathrm{E}_K^{1,i}(M_i')$; $X_i \leftarrow M_i' \oplus \mathrm{E}_K^{0,0}(W_i)$ **od**
225 **if** $d = 0$ **then** $X \leftarrow X_1 \oplus \cdots \oplus X_m \oplus \mathbf{0}$ **else if** $d \leq 127$ **then** $X \leftarrow X_1 \oplus \cdots \oplus X_m \oplus \mathrm{E}_K^{0,4}(M_{\mathsf{u}}10^*)$
226 **else** $X \leftarrow X_1 \oplus \cdots \oplus X_m \oplus \mathrm{E}_K^{0,4}(M_{\mathsf{u}}) \oplus \mathrm{E}_K^{0,5}(M_{\mathsf{v}}10^*)$ **fi**
227 $S_{\mathsf{x}} \leftarrow M_{\mathsf{x}} \oplus \Delta \oplus X \oplus \mathrm{E}_K^{0,1}(M_{\mathsf{y}})$; $S_{\mathsf{y}} \leftarrow M_{\mathsf{y}} \oplus \mathrm{E}_K^{-1,1}(S_{\mathsf{x}})$; $S \leftarrow S_{\mathsf{x}} \oplus S_{\mathsf{y}}$
228 **for** $i \leftarrow 1$ **to** m **do** $S' \leftarrow \mathrm{E}_K^{2,i}(S)$; $Y_i \leftarrow W_i \oplus S'$; $Z_i \leftarrow X_i \oplus S'$; $C_i' \leftarrow Y_i \oplus \mathrm{E}_K^{0,0}(Z_i)$; $C_i \leftarrow Z_i \oplus \mathrm{E}_K^{1,i}(C_i')$ **od**
229 **if** $d = 0$ **then** $C_{\mathsf{u}} \leftarrow C_{\mathsf{v}} \leftarrow \varepsilon$; $Y \leftarrow Y_1 \oplus \cdots \oplus Y_m \oplus \mathbf{0}$
230 **else if** $d \leq 127$ **then** $C_{\mathsf{u}} \leftarrow M_{\mathsf{u}} \oplus \mathrm{E}_K^{-1,4}(S)$; $C_{\mathsf{v}} \leftarrow \varepsilon$; $Y \leftarrow Y_1 \oplus \cdots \oplus Y_m \oplus \mathrm{E}_K^{0,4}(C_{\mathsf{u}}10^*)$
231 **else** $C_{\mathsf{u}} \leftarrow M_{\mathsf{u}} \oplus \mathrm{E}_K^{-1,4}(S)$; $C_{\mathsf{v}} \leftarrow M_{\mathsf{v}} \oplus \mathrm{E}_K^{-1,5}(S)$; $Y \leftarrow Y_1 \oplus \cdots \oplus Y_m \oplus \mathrm{E}_K^{0,4}(C_{\mathsf{u}}) \oplus \mathrm{E}_K^{0,5}(C_{\mathsf{v}}10^*)$ **fi**
232 $C_{\mathsf{y}} \leftarrow S_{\mathsf{x}} \oplus \mathrm{E}_K^{-1,2}(S_{\mathsf{y}})$; $C_{\mathsf{x}} \leftarrow S_{\mathsf{y}} \oplus \Delta \oplus Y \oplus \mathrm{E}_K^{0,2}(C_{\mathsf{y}})$
233 **return** $C_1 C_1' \cdots C_m C_m'$ $C_{\mathsf{u}} C_{\mathsf{v}}$ $C_{\mathsf{x}} C_{\mathsf{y}}$

300 **algorithm** AEZ-hash$(K, \boldsymbol{T})$ // AXU hash. T is a vector of strings
301 $(T_1, \ldots, T_t) \leftarrow \boldsymbol{T}$
302 **for** $i \leftarrow 1$ **to** t **do**
303 $\quad \ell \leftarrow \max(1, \lceil |T_i|/128 \rceil)$; $j \leftarrow i+2$; $Z_1 \cdots Z_\ell \leftarrow T_i$ where $|Z_1| = \cdots = |Z_{\ell-1}| = 128$
304 $\quad$ **if** $|Z_\ell| = 128$ **then** $\Delta_i \leftarrow \mathrm{E}_K^{j,1}(Z_1) \oplus \cdots \oplus \mathrm{E}_K^{j,\ell}(Z_\ell)$ **fi**
305 $\quad$ **if** $|Z_\ell| < 128$ **then** $\Delta_i \leftarrow \mathrm{E}_K^{j,1}(Z_1) \oplus \cdots \oplus \mathrm{E}_K^{j,\ell-1}(Z_{\ell-1}) \oplus \mathrm{E}_K^{j,0}(Z_\ell 10^*)$ **fi**
306 **return** $\Delta_1 \oplus \cdots \oplus \Delta_t \oplus \mathbf{0}$

310 **algorithm** AEZ-prf$(K, \boldsymbol{T}, \tau)$ // PRF used when $M = \varepsilon$
311 $\Delta \leftarrow$ AEZ-hash$(K, \boldsymbol{T})$
312 **return** $(\mathrm{E}_K^{-1,3}(\Delta) \,\|\, \mathrm{E}_K^{-1,3}(\Delta \oplus [1]_{128}) \,\|\, \mathrm{E}_K^{-1,3}(\Delta \oplus [2]_{128}) \,\|\, \cdots)[1..\tau]$

400 **algorithm** $\mathrm{E}_K^{j,i}(X)$ // Scaled-down TBC
401 $I \,\|\, J \,\|\, L \leftarrow$ Extract(K) where $|I| = |J| = |L| = 128$
402 $\boldsymbol{K} \leftarrow (\mathbf{0}, I, J, L, I, J, L, I, J, L, I)$; $\boldsymbol{k} \leftarrow (\mathbf{0}, J, I, L, \mathbf{0})$
403 **if** $j = -1$ **then** $\Delta \leftarrow i \cdot L$; **return** AES10$_{\boldsymbol{K}}(X \oplus \Delta)$ **fi**
404 $\Delta \leftarrow j \cdot J \oplus 2^{\lfloor i/8 \rfloor} \cdot I \oplus (i \bmod 8) \cdot L$
405 **return** AES4$_{\boldsymbol{k}}(X \oplus \Delta)$

410 **algorithm** Extract(K) // Map key to subkeys
411 **if** $|K| = 384$ **then return** K
412 **else return** BLAKE2b(K)

600 **algorithm** Decipher$(K, \boldsymbol{T}, C)$ // AEZ deciphering
601 **if** $|C| < 256$ **then return** Decipher-AEZ-tiny$(K, \boldsymbol{T}, C)$
602 **if** $|C| \geq 256$ **then return** Decipher-AEZ-core$(K, \boldsymbol{T}, C)$

610 **algorithm** Decipher-AEZ-tiny$(K, \boldsymbol{T}, C)$ // AEZ-tiny deciphering
611 $\mu \leftarrow |C|$; $n \leftarrow \mu/2$; $\Delta \leftarrow$ AEZ-hash$(K, \boldsymbol{T})$
612 **if** $\mu < 128$ **then** $C \leftarrow C \oplus (\mathrm{E}_K^{0,3}(\Delta \oplus (C0^* \vee 10^*)) \wedge 10^*)$ **fi**
613 **if** $\mu = 8$ **then** $k \leftarrow 24$ **else if** $\mu = 16$ **then** $k \leftarrow 16$ **else if** $\mu < 128$ **then** $k \leftarrow 10$ **else** $k \leftarrow 8$ **fi**
614 $L \leftarrow C[1\,..\,n]$; $R \leftarrow C[n+1\,..\,\mu]$; **if** $\mu \geq 128$ **then** $i \leftarrow 6$ **else** $i \leftarrow 7$ **fi**
615 **for** $j \leftarrow k-1$ **downto** 0 **do** $R' \leftarrow L \oplus ((\mathrm{E}_K^{0,i}(\Delta \oplus R10^* \oplus [j]_{128}))[1\,..\,n])$; $L \leftarrow R$; $R \leftarrow R'$ **od**
616 $M \leftarrow R \,\|\, L$; **return** M

620 **algorithm** Decipher-AEZ-core$(K, \boldsymbol{T}, C)$ // AEZ-core deciphering
621 $\Delta \leftarrow$ AEZ-hash$(K, \boldsymbol{T})$
622 $C_1 C_1' \cdots C_m C_m'$ C_{uv} $C_{\mathsf{x}} C_{\mathsf{y}} \leftarrow C$ where $|C_1| = \cdots = |C_m'| = |C_{\mathsf{x}}| = |C_{\mathsf{y}}| = 128$ and $|C_{\mathsf{uv}}| < 256$
623 $d \leftarrow |C_{\mathsf{uv}}|$; **if** $d \leq 127$ **then** $C_{\mathsf{u}} \leftarrow C_{\mathsf{uv}}$; $C_{\mathsf{v}} \leftarrow \varepsilon$ **else** $C_{\mathsf{u}} \leftarrow C_{\mathsf{uv}}[1..128]$; $C_{\mathsf{v}} \leftarrow C_{\mathsf{uv}}[129..|C_{\mathsf{uv}}|]$ **fi**
624 **for** $i \leftarrow 1$ **to** m **do** $W_i \leftarrow C_i \oplus \mathrm{E}_K^{1,i}(C_i')$; $Y_i \leftarrow C_i' \oplus \mathrm{E}_K^{0,0}(W_i)$ **od**
625 **if** $d = 0$ **then** $Y \leftarrow Y_1 \oplus \cdots \oplus Y_m \oplus \mathbf{0}$ **else if** $d \leq 127$ **then** $Y \leftarrow Y_1 \oplus \cdots \oplus Y_m \oplus \mathrm{E}_K^{0,4}(C_{\mathsf{u}}10^*)$
626 **else** $Y \leftarrow Y_1 \oplus \cdots \oplus Y_m \oplus \mathrm{E}_K^{0,4}(C_{\mathsf{u}}) \oplus \mathrm{E}_K^{0,5}(C_{\mathsf{v}}10^*)$ **fi**
627 $S_{\mathsf{x}} \leftarrow C_{\mathsf{x}} \oplus \Delta \oplus Y \oplus \mathrm{E}_K^{0,2}(C_{\mathsf{y}})$; $S_{\mathsf{y}} \leftarrow C_{\mathsf{y}} \oplus \mathrm{E}_K^{-1,2}(S_{\mathsf{x}})$; $S \leftarrow S_{\mathsf{x}} \oplus S_{\mathsf{y}}$
628 **for** $i \leftarrow 1$ **to** m **do** $S' \leftarrow \mathrm{E}_K^{2,i}(S)$; $X_i \leftarrow W_i \oplus S'$; $Z_i \leftarrow Y_i \oplus S'$; $M_i' \leftarrow X_i \oplus \mathrm{E}_K^{0,0}(Z_i)$; $M_i \leftarrow Z_i \oplus \mathrm{E}_K^{1,i}(M_i')$ **od**
629 **if** $d = 0$ **then** $M_{\mathsf{u}} \leftarrow M_{\mathsf{v}} \leftarrow \varepsilon$; $X \leftarrow X_1 \oplus \cdots \oplus X_m \oplus \mathbf{0}$
630 **else if** $d \leq 127$ **then** $M_{\mathsf{u}} \leftarrow C_{\mathsf{u}} \oplus \mathrm{E}_K^{-1,4}(S)$; $M_{\mathsf{v}} \leftarrow \varepsilon$; $X \leftarrow X_1 \oplus \cdots \oplus X_m \oplus \mathrm{E}_K^{0,4}(M_{\mathsf{u}}10^*)$
631 **else** $M_{\mathsf{u}} \leftarrow C_{\mathsf{u}} \oplus \mathrm{E}_K^{-1,4}(S)$; $M_{\mathsf{v}} \leftarrow C_{\mathsf{v}} \oplus \mathrm{E}_K^{-1,5}(S)$; $X \leftarrow X_1 \oplus \cdots \oplus X_m \oplus \mathrm{E}_K^{0,4}(M_{\mathsf{u}}) \oplus \mathrm{E}_K^{0,5}(M_{\mathsf{v}}10^*)$ **fi**
632 $M_{\mathsf{y}} \leftarrow S_{\mathsf{x}} \oplus \mathrm{E}_K^{-1,1}(S_{\mathsf{y}})$; $M_{\mathsf{x}} \leftarrow S_{\mathsf{y}} \oplus \Delta \oplus X \oplus \mathrm{E}_K^{0,1}(M_{\mathsf{y}})$
633 **return** $M_1 M_1' \cdots M_m M_m'$ $M_{\mathsf{u}} M_{\mathsf{v}}$ $M_{\mathsf{x}} M_{\mathsf{y}}$

AEZ in details

100 **algorithm** Encrypt$(K, N, \boldsymbol{A}, \tau, M)$ // AEZ authenticated encryption
101 $X \leftarrow M \,\|\, 0^\tau$; $(A_1, \ldots, A_a) \leftarrow \boldsymbol{A}$
102 $\boldsymbol{T} \leftarrow ([\tau]_{128}, N, A_1, \ldots, A_a)$
103 **if** $M = \varepsilon$ **then return** AEZ-prf$(K, \boldsymbol{T}, \tau)$
104 **return** Encipher$(K, \boldsymbol{T}, X)$

110 **algorithm** Decrypt$(K, N, \boldsymbol{A}, \tau, C)$ // AEZ authenticated decryption
111 $(A_1, \ldots, A_a) \leftarrow \boldsymbol{A}$; $\boldsymbol{T} \leftarrow ([\tau]_{128}, N, A_1, \ldots, A_a)$
112 **if** $|C| < \tau$ **then return** $\perp$
113 **if** $|C| = \tau$ **then if** $C =$ AEZ-prf$(K, \boldsymbol{T}, \tau)$ **then return** ε **else return** $\perp$ **fi fi**
114 $X \leftarrow$ Decipher$(K, \boldsymbol{T}, C)$
115 $M \,\|\, Z \leftarrow X$ where $|Z| = \tau$
116 **if** $(Z = 0^\tau)$ **then return** M **else return** $\perp$

200 **algorithm** Encipher$(K, \boldsymbol{T}, X)$ // AEZ enciphering
201 **if** $|X| < 256$ **then return** Encipher-AEZ-tiny$(K, \boldsymbol{T}, X)$
202 **if** $|X| \geq 256$ **then return** Encipher-AEZ-core$(K, \boldsymbol{T}, X)$

210 **algorithm** Encipher-AEZ-tiny$(K, \boldsymbol{T}, M)$ // AEZ-tiny enciphering
211 $\mu \leftarrow |M|$; $n \leftarrow \mu/2$; $\Delta \leftarrow$ AEZ-hash$(K, \boldsymbol{T})$
212 **if** $\mu = 8$ **then** $k \leftarrow 24$ **else if** $\mu = 16$ **then** $k \leftarrow 16$ **else if** $\mu < 128$ **then** $k \leftarrow 10$ **else** $k \leftarrow 8$ **fi**
213 $L \leftarrow M[1\,..\,n]$; $R \leftarrow M[n+1\,..\,\mu]$; **if** $\mu \geq 128$ **then** $i \leftarrow 6$ **else** $i \leftarrow 7$ **fi**
214 **for** $j \leftarrow 0$ **to** $k-1$ **do** $R' \leftarrow L \oplus ((\mathrm{E}_K^{0,i}(\Delta \oplus R10^* \oplus [j]_{128}))[1\,..\,n])$; $L \leftarrow R$; $R \leftarrow R'$ **od**
215 $C \leftarrow R \,\|\, L$; **if** $\mu < 128$ **then** $C \leftarrow C \oplus (\mathrm{E}_K^{0,3}(\Delta \oplus (C0^* \vee 10^*)) \wedge 10^*)$ **fi**
216 **return** C

220 **algorithm** Encipher-AEZ-core$(K, \boldsymbol{T}, M)$ // AEZ-core enciphering
221 $\Delta \leftarrow$ AEZ-hash$(K, \boldsymbol{T})$
222 $M_1 M_1' \cdots M_m M_m'$ M_{uv} $M_{\mathsf{x}} M_{\mathsf{y}} \leftarrow M$ where $|M_1| = \cdots = |M_m'| = |M_{\mathsf{x}}| = |M_{\mathsf{y}}| = 128$ and $|M_{\mathsf{uv}}| < 256$
223 $d \leftarrow |M_{\mathsf{uv}}|$; **if** $d \leq 127$ **then** $M_{\mathsf{u}} \leftarrow M_{\mathsf{uv}}$; $M_{\mathsf{v}} \leftarrow \varepsilon$ **else** $M_{\mathsf{u}} \leftarrow M_{\mathsf{uv}}[1..128]$; $M_{\mathsf{v}} \leftarrow M_{\mathsf{uv}}[129..|M_{\mathsf{uv}}|]$ **fi**
224 **for** $i \leftarrow 1$ **to** m **do** $W_i \leftarrow M_i \oplus \mathrm{E}_K^{1,i}(M_i')$; $X_i \leftarrow M_i' \oplus \mathrm{E}_K^{0,0}(W_i)$ **od**
225 **if** $d = 0$ **then** $X \leftarrow X_1 \oplus \cdots \oplus X_m \oplus \mathbf{0}$ **else if** $d \leq 127$ **then** $X \leftarrow X_1 \oplus \cdots \oplus X_m \oplus \mathrm{E}_K^{0,4}(M_{\mathsf{u}}10^*)$
226 **else** $X \leftarrow X_1 \oplus \cdots \oplus X_m \oplus \mathrm{E}_K^{0,4}(M_{\mathsf{u}}) \oplus \mathrm{E}_K^{0,5}(M_{\mathsf{v}}10^*)$ **fi**
227 $S_{\mathsf{x}} \leftarrow M_{\mathsf{x}} \oplus \Delta \oplus X \oplus \mathrm{E}_K^{0,1}(M_{\mathsf{y}})$; $S_{\mathsf{y}} \leftarrow M_{\mathsf{y}} \oplus \mathrm{E}_K^{-1,1}(S_{\mathsf{x}})$; $S \leftarrow S_{\mathsf{x}} \oplus S_{\mathsf{y}}$
228 **for** $i \leftarrow 1$ **to** m **do** $S' \leftarrow \mathrm{E}_K^{2,i}(S)$; $Y_i \leftarrow W_i \oplus S'$; $Z_i \leftarrow X_i \oplus S'$; $C_i' \leftarrow Y_i \oplus \mathrm{E}_K^{0,0}(Z_i)$; $C_i \leftarrow Z_i \oplus \mathrm{E}_K^{1,i}(C_i')$ **od**
229 **if** $d = 0$ **then** $C_{\mathsf{u}} \leftarrow C_{\mathsf{v}} \leftarrow \varepsilon$; $Y \leftarrow Y_1 \oplus \cdots \oplus Y_m \oplus \mathbf{0}$
230 **else if** $d \leq 127$ **then** $C_{\mathsf{u}} \leftarrow M_{\mathsf{u}} \oplus \mathrm{E}_K^{-1,4}(S)$; $C_{\mathsf{v}} \leftarrow \varepsilon$; $Y \leftarrow Y_1 \oplus \cdots \oplus Y_m \oplus \mathrm{E}_K^{0,4}(C_{\mathsf{u}}10^*)$
231 **else** $C_{\mathsf{u}} \leftarrow M_{\mathsf{u}} \oplus \mathrm{E}_K^{-1,4}(S)$; $C_{\mathsf{v}} \leftarrow M_{\mathsf{v}} \oplus \mathrm{E}_K^{-1,5}(S)$; $Y \leftarrow Y_1 \oplus \cdots \oplus Y_m \oplus \mathrm{E}_K^{0,4}(C_{\mathsf{u}}) \oplus \mathrm{E}_K^{0,5}(C_{\mathsf{v}}10^*)$ **fi**
232 $C_{\mathsf{y}} \leftarrow S_{\mathsf{x}} \oplus \mathrm{E}_K^{-1,2}(S_{\mathsf{y}})$; $C_{\mathsf{x}} \leftarrow S_{\mathsf{y}} \oplus \Delta \oplus Y \oplus \mathrm{E}_K^{0,2}(C_{\mathsf{y}})$
233 **return** $C_1 C_1' \cdots C_m C_m'$ $C_{\mathsf{u}} C_{\mathsf{v}}$ $C_{\mathsf{x}} C_{\mathsf{y}}$

300 **algorithm** AEZ-hash$(K, \boldsymbol{T})$ // AXU hash. T is a vector of strings
301 $(T_1, \ldots, T_t) \leftarrow \boldsymbol{T}$
302 **for** $i \leftarrow 1$ **to** t **do**
303 $\quad \ell \leftarrow \max(1, \lceil |T_i|/128 \rceil)$; $j \leftarrow i+2$; $Z_1 \cdots Z_\ell \leftarrow T_i$ where $|Z_1| = \cdots = |Z_{\ell-1}| = 128$
304 $\quad$ **if** $|Z_\ell| = 128$ **then** $\Delta_i \leftarrow \mathrm{E}_K^{j,1}(Z_1) \oplus \cdots \oplus \mathrm{E}_K^{j,\ell}(Z_\ell)$ **fi**
305 $\quad$ **if** $|Z_\ell| < 128$ **then** $\Delta_i \leftarrow \mathrm{E}_K^{j,1}(Z_1) \oplus \cdots \oplus \mathrm{E}_K^{j,\ell-1}(Z_{\ell-1}) \oplus \mathrm{E}_K^{j,0}(Z_\ell 10^*)$ **fi**
306 **return** $\Delta_1 \oplus \cdots \oplus \Delta_t \oplus \mathbf{0}$

310 **algorithm** AEZ-prf$(K, \boldsymbol{T}, \tau)$ // PRF used when $M = \varepsilon$
311 $\Delta \leftarrow$ AEZ-hash$(K, \boldsymbol{T})$
312 **return** $(\mathrm{E}_K^{-1,3}(\Delta) \,\|\, \mathrm{E}_K^{-1,3}(\Delta \oplus [1]_{128}) \,\|\, \mathrm{E}_K^{-1,3}(\Delta \oplus [2]_{128}) \,\|\, \cdots)[1..\tau]$

400 **algorithm** $\mathrm{E}_K^{j,i}(X)$ // Scaled-down TBC
401 $I \,\|\, J \,\|\, L \leftarrow$ Extract(K) where $|I| = |J| = |L| = 128$
402 $\boldsymbol{K} \leftarrow (\mathbf{0}, I, J, L, I, J, L, I, J, L, I)$; $\boldsymbol{k} \leftarrow (\mathbf{0}, J, I, L, \mathbf{0})$
403 **if** $j = -1$ **then** $\Delta \leftarrow i \cdot L$; **return** AES10$_{\boldsymbol{K}}(X \oplus \Delta)$ **fi**
404 $\Delta \leftarrow j \cdot J \oplus 2^{\lceil i/8 \rceil} \cdot I \oplus (i \bmod 8) \cdot L$
405 **return** AES4$_{\boldsymbol{k}}(X \oplus \Delta)$

410 **algorithm** Extract(K) // Map key to subkeys
411 **if** $|K| = 384$ **then return** K
412 **else return** BLAKE2b(K)

600 **algorithm** Decipher$(K, \boldsymbol{T}, C)$ // AEZ deciphering
601 **if** $|C| < 256$ **then return** Decipher-AEZ-tiny$(K, \boldsymbol{T}, C)$
602 **if** $|C| \geq 256$ **then return** Decipher-AEZ-core$(K, \boldsymbol{T}, C)$

610 **algorithm** Decipher-AEZ-tiny$(K, \boldsymbol{T}, C)$ // AEZ-tiny deciphering
611 $\mu \leftarrow |C|$; $n \leftarrow \mu/2$; $\Delta \leftarrow$ AEZ-hash$(K, \boldsymbol{T})$
612 **if** $\mu < 128$ **then** $C \leftarrow C \oplus (\mathrm{E}_K^{0,3}(\Delta \oplus (C0^* \vee 10^*)) \wedge 10^*)$ **fi**
613 **if** $\mu = 8$ **then** $k \leftarrow 24$ **else if** $\mu = 16$ **then** $k \leftarrow 16$ **else if** $\mu < 128$ **then** $k \leftarrow 10$ **else** $k \leftarrow 8$ **fi**
614 $L \leftarrow C[1\,..\,n]$; $R \leftarrow C[n+1\,..\,\mu]$; **if** $\mu \geq 128$ **then** $i \leftarrow 6$ **else** $i \leftarrow 7$ **fi**
615 **for** $j \leftarrow k-1$ **downto** 0 **do** $R' \leftarrow L \oplus ((\mathrm{E}_K^{0,i}(\Delta \oplus R10^* \oplus [j]_{128}))[1\,..\,n])$; $L \leftarrow R$; $R \leftarrow R'$ **od**
616 $M \leftarrow R \,\|\, L$; **return** M

620 **algorithm** Decipher-AEZ-core$(K, \boldsymbol{T}, C)$ // AEZ-core deciphering
621 $\Delta \leftarrow$ AEZ-hash$(K, \boldsymbol{T})$
622 $C_1 C_1' \cdots C_m C_m'$ C_{uv} $C_{\mathsf{x}} C_{\mathsf{y}} \leftarrow C$ where $|C_1| = \cdots = |C_m'| = |C_{\mathsf{x}}| = |C_{\mathsf{y}}| = 128$ and $|C_{\mathsf{uv}}| < 256$
623 $d \leftarrow |C_{\mathsf{uv}}|$; **if** $d \leq 127$ **then** $C_{\mathsf{u}} \leftarrow C_{\mathsf{uv}}$; $C_{\mathsf{v}} \leftarrow \varepsilon$ **else** $C_{\mathsf{u}} \leftarrow C_{\mathsf{uv}}[1..128]$; $C_{\mathsf{v}} \leftarrow C_{\mathsf{uv}}[129..|C_{\mathsf{uv}}|]$ **fi**
624 **for** $i \leftarrow 1$ **to** m **do** $W_i \leftarrow C_i \oplus \mathrm{E}_K^{1,i}(C_i')$; $Y_i \leftarrow C_i' \oplus \mathrm{E}_K^{0,0}(W_i)$ **od**
625 **if** $d = 0$ **then** $Y \leftarrow Y_1 \oplus \cdots \oplus Y_m \oplus \mathbf{0}$ **else if** $d \leq 127$ **then** $Y \leftarrow Y_1 \oplus \cdots \oplus Y_m \oplus \mathrm{E}_K^{0,4}(C_{\mathsf{u}}10^*)$
626 **else** $Y \leftarrow Y_1 \oplus \cdots \oplus Y_m \oplus \mathrm{E}_K^{0,4}(C_{\mathsf{u}}) \oplus \mathrm{E}_K^{0,5}(C_{\mathsf{v}}10^*)$ **fi**
627 $S_{\mathsf{x}} \leftarrow C_{\mathsf{x}} \oplus \Delta \oplus Y \oplus \mathrm{E}_K^{0,2}(C_{\mathsf{y}})$; $S_{\mathsf{y}} \leftarrow C_{\mathsf{y}} \oplus \mathrm{E}_K^{-1,2}(S_{\mathsf{x}})$; $S \leftarrow S_{\mathsf{x}} \oplus S_{\mathsf{y}}$
628 **for** $i \leftarrow 1$ **to** m **do** $S' \leftarrow \mathrm{E}_K^{2,i}(S)$; $X_i \leftarrow W_i \oplus S'$; $Z_i \leftarrow Y_i \oplus S'$; $M_i' \leftarrow X_i \oplus \mathrm{E}_K^{0,0}(Z_i)$; $M_i \leftarrow Z_i \oplus \mathrm{E}_K^{1,i}(M_i')$ **od**
629 **if** $d = 0$ **then** $M_{\mathsf{u}} \leftarrow M_{\mathsf{v}} \leftarrow \varepsilon$; $X \leftarrow X_1 \oplus \cdots \oplus X_m \oplus \mathbf{0}$
630 **else if** $d \leq 127$ **then** $M_{\mathsf{u}} \leftarrow C_{\mathsf{u}} \oplus \mathrm{E}_K^{-1,4}(S)$; $M_{\mathsf{v}} \leftarrow \varepsilon$; $X \leftarrow X_1 \oplus \cdots \oplus X_m \oplus \mathrm{E}_K^{0,4}(M_{\mathsf{u}}10^*)$
631 **else** $M_{\mathsf{u}} \leftarrow C_{\mathsf{u}} \oplus \mathrm{E}_K^{-1,4}(S)$; $M_{\mathsf{v}} \leftarrow C_{\mathsf{v}} \oplus \mathrm{E}_K^{-1,5}(S)$; $X \leftarrow X_1 \oplus \cdots \oplus X_m \oplus \mathrm{E}_K^{0,4}(M_{\mathsf{u}}) \oplus \mathrm{E}_K^{0,5}(M_{\mathsf{v}}10^*)$ **fi**
632 $M_{\mathsf{y}} \leftarrow S_{\mathsf{x}} \oplus \mathrm{E}_K^{-1,1}(S_{\mathsf{y}})$; $M_{\mathsf{x}} \leftarrow S_{\mathsf{y}} \oplus \Delta \oplus X \oplus \mathrm{E}_K^{0,1}(M_{\mathsf{y}})$
633 **return** $M_1 M_1' \cdots M_m M_m'$ $M_{\mathsf{u}} M_{\mathsf{v}}$ $M_{\mathsf{x}} M_{\mathsf{y}}$

Call to AEZ

Encrypt(K, A, M)

K : Secret key, 3 128-bit blocks (I, J, L),

A : Additional data, arbitrary-length vector of elements with an arbitrary number of 128-bit blocks $((\text{block}^*)^*)$, noted A_i^j,

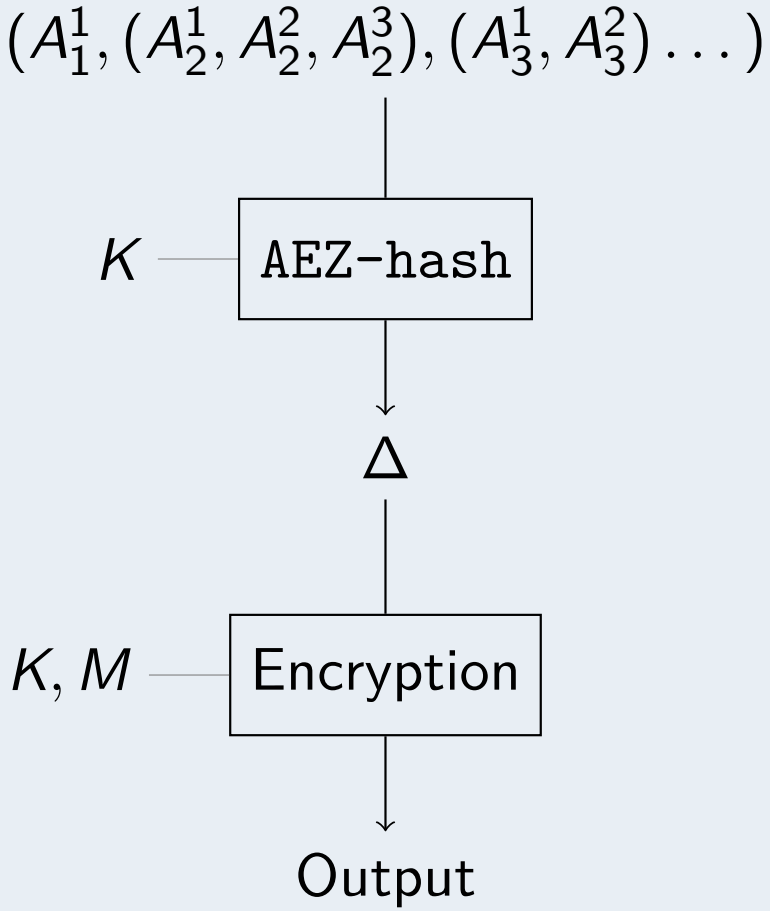
M : Message to be encrypted, of arbitrary length (block^*).

Constraints

- A_1 is the authenticator length (the output length overhead) τ,
- A_2 is the nonce N.

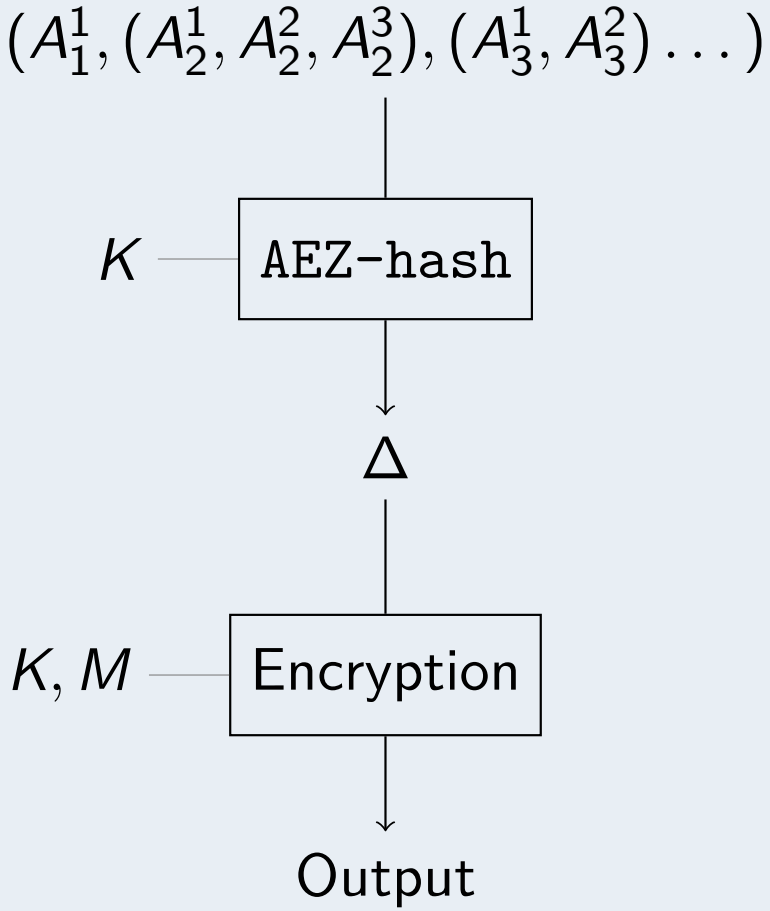
Authenticating the additional data

Encrypt(K, A, M)

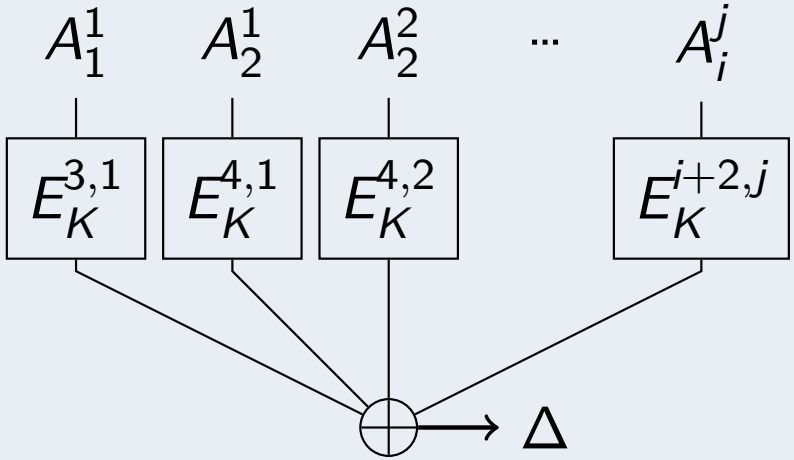


Authenticating the additional data

Encrypt(K, A, M)

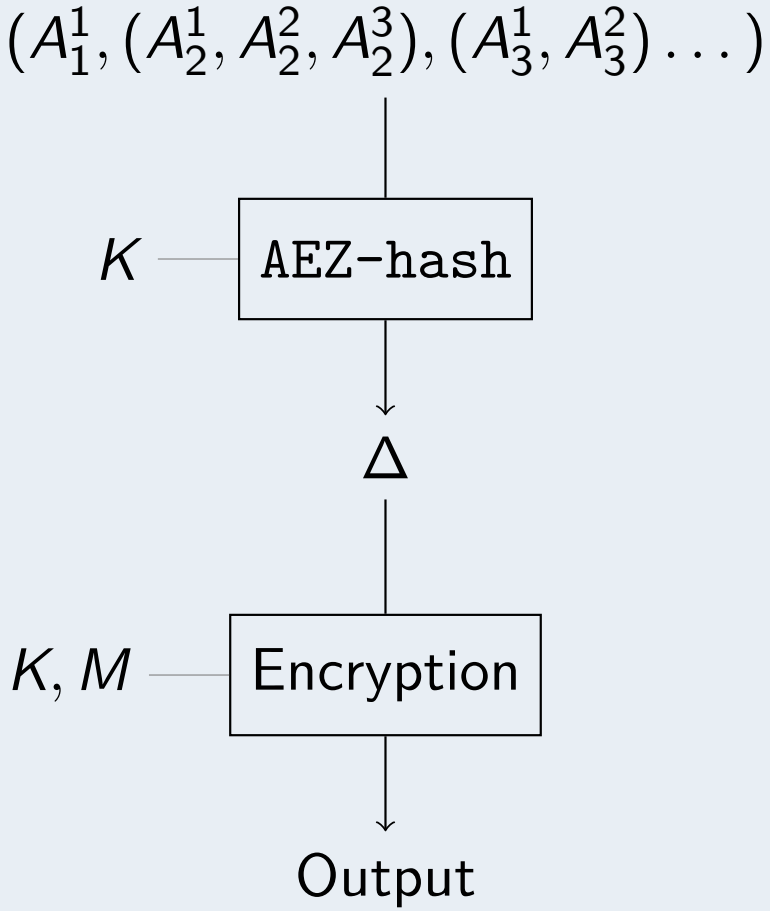


AEZ-hash

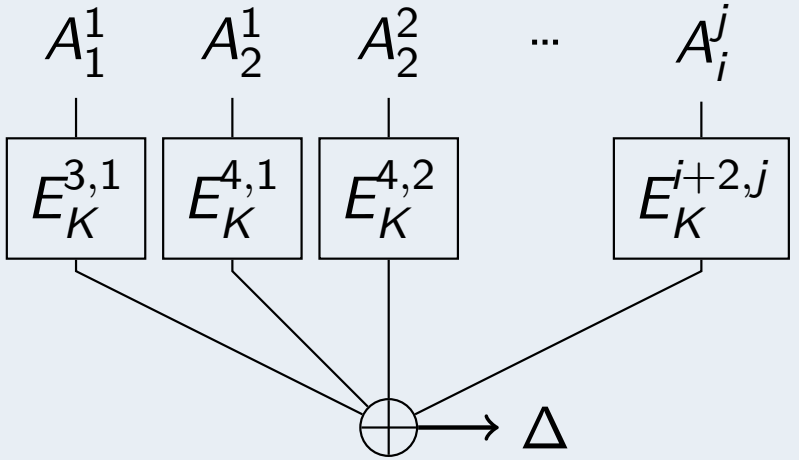


Authenticating the additional data

Encrypt(K, A, M)



AEZ-hash



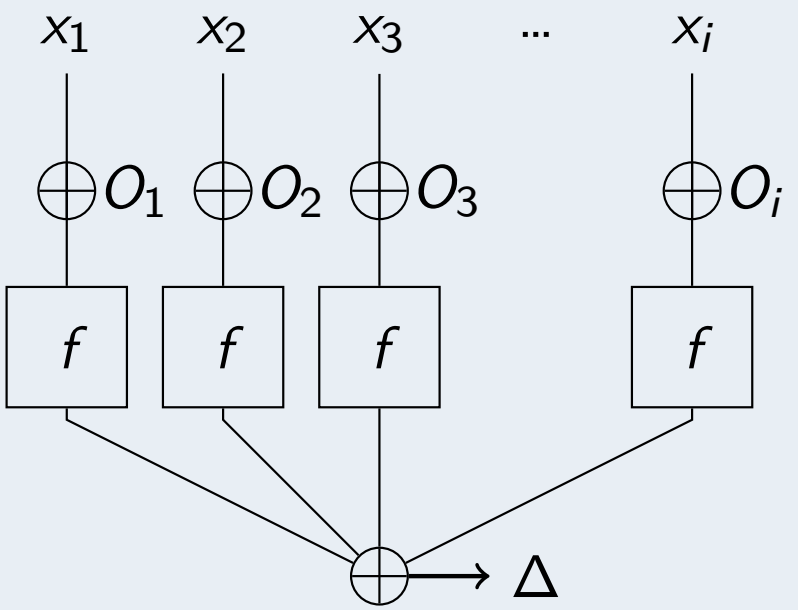
$E_K^{i,j}(A_\ell^m)$ (in AEZv5)

$K = I, J, L$

$\mathtt{AES4}(A_\ell^m \oplus iJ \oplus 2^{\lceil j/8 \rceil} I \oplus (j \bmod 8)L)$

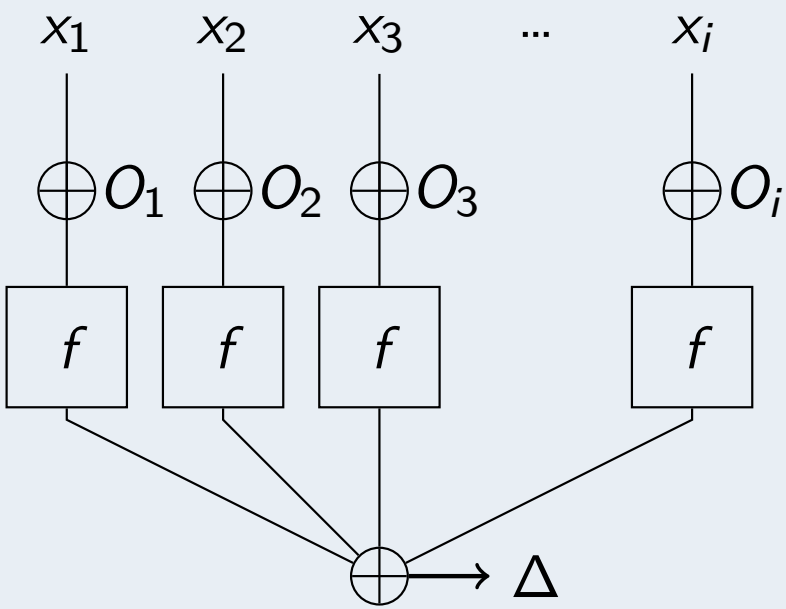
An interesting property [CG16]

AEZ-hash

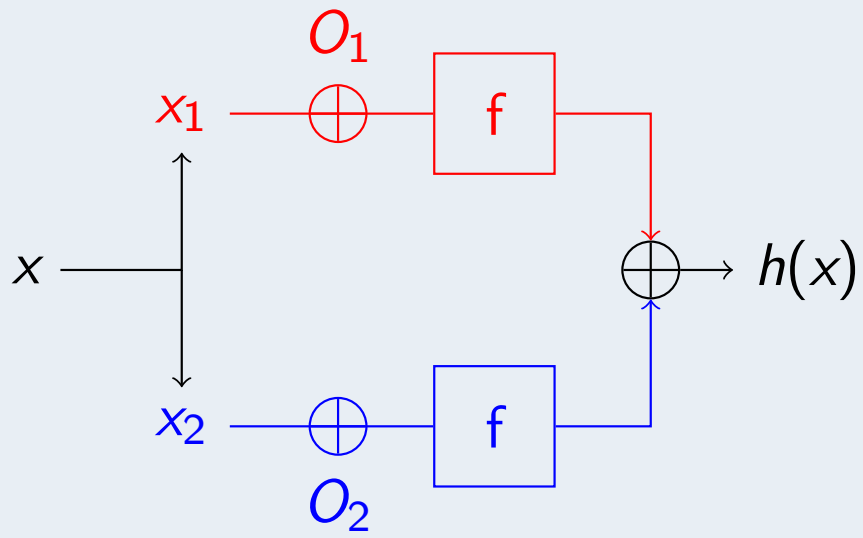


An interesting property [CG16]

AEZ-hash



With identical inputs



If $x' = x \oplus O_1 \oplus O_2$, then $h(x) = h(x')$.

We can learn $O_1 \oplus O_2$ thanks to a collision!

Diving into the offsets

$A_i^j : O_{i+2}^j = (i+2)J \oplus 2^{\lceil j/8 \rceil} I \oplus (j \bmod 8)L$

Find the collisions by trying many associated data (τ, A_2^1, A_3^1) with $A_2^1 = A_3^1$

$A_2^1 : O_4^1 = 4J \oplus 8I \oplus L$

$A_3^1 : O_5^1 = 5J \oplus 8I \oplus L$

A collision retrieves $O_4^1 \oplus O_5^1 = J$.

We can determine J from a collision in $f_J(x) = \text{Encrypt}(K, (\tau, x, x), \epsilon)$.

The analysis

- Searching collisions with AD (τ, x, x).
- Same idea for I : $(\tau, N, (x, A, B, C, D, E, F, G, x))$,
- and L : $(\tau, N, (x, x))$,
- key-recovery for I and L uses a fixed nonce, J uses any nonce.

Collisions at the birthday bound : needs around 2^{68} blocks processed. But the security is only claimed up to 2^{44} blocks.

Quantum attacks

Asymetric cryptography

- Attacks on some asymetric schemes (Q1) [Shor97]

Symetric cryptography

- Quadratic gain on exhaustive search (Q1) [Grover96]
- Dedicated attack on Even-Mansour scheme (Q2) [KM12]
- AE & Quantum slide attacks (Q2) [KLLN16]

Quantum attack

Collision property of AEZ

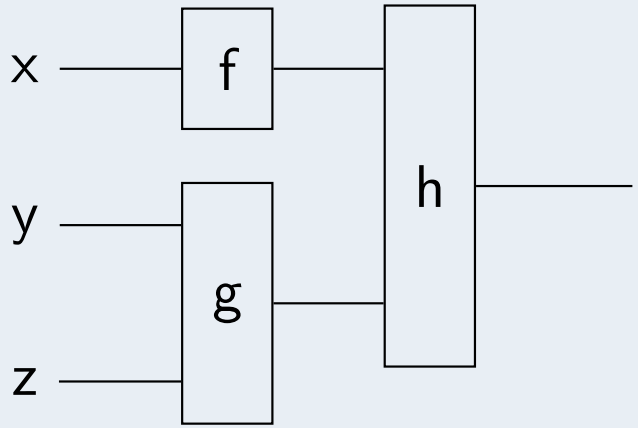
$f(x) = f(x')$ with $x \oplus x'$ a subkey.

Attack principles

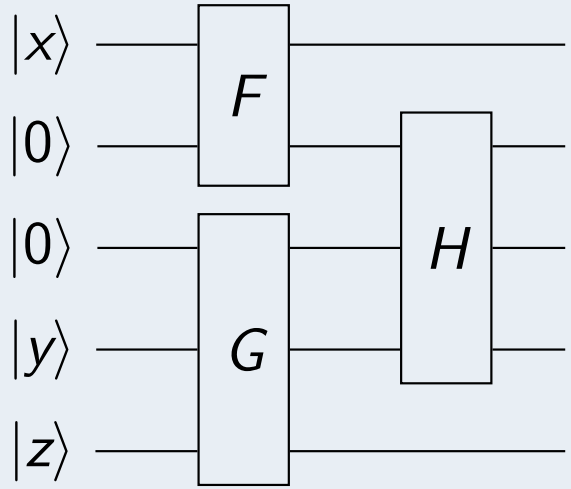
Use the property $f(x) = f(x \oplus s)$ more efficiently, with Simon's algorithm.

Quantum computing

Classical computing



Quantum computing



Differences

- Reversible computation
- Superposition (NOT parallelism)

Superposition

Measurement

State $|0001\rangle \quad \frac{1}{\sqrt{3}}|0110\rangle - \frac{1}{\sqrt{3}}|0101\rangle + \frac{1}{\sqrt{3}}|0001\rangle$

Superposition

Measurement		
State	$\|0001\rangle$	$\frac{1}{\sqrt{3}}\|0110\rangle - \frac{1}{\sqrt{3}}\|0101\rangle + \frac{1}{\sqrt{3}}\|0001\rangle$
Measurement (all qubits)	0001	0110 ($\frac{1}{3}$) or 0101 ($\frac{1}{3}$) or 0001 ($\frac{1}{3}$)
New state	$\|0001\rangle$	$\|0110\rangle$ or $\|0101\rangle$ or $\|0001\rangle$

Superposition

Measurement		
State	$\|0001\rangle$	$\frac{1}{\sqrt{3}}\|0110\rangle - \frac{1}{\sqrt{3}}\|0101\rangle + \frac{1}{\sqrt{3}}\|0001\rangle$
Measurement (first qubit)	0	0
New state	$\|0001\rangle$	$\frac{1}{\sqrt{3}}\|0110\rangle - \frac{1}{\sqrt{3}}\|0101\rangle + \frac{1}{\sqrt{3}}\|0001\rangle$

Superposition

Measurement		
State	$\|0001\rangle$	$\frac{1}{\sqrt{3}}\|0110\rangle - \frac{1}{\sqrt{3}}\|0101\rangle + \frac{1}{\sqrt{3}}\|0001\rangle$
Measurement (second qubit)	0	1 ($\frac{2}{3}$) or 0 ($\frac{1}{3}$)
New state	$\|0001\rangle$	$\frac{1}{\sqrt{2}}\|0110\rangle - \frac{1}{\sqrt{2}}\|0101\rangle$ or $\|0001\rangle$

Superposition

Measurement		
State	$\|0001\rangle$	$\frac{1}{\sqrt{3}}\|0110\rangle - \frac{1}{\sqrt{3}}\|0101\rangle + \frac{1}{\sqrt{3}}\|0001\rangle$
Measurement (third qubit)	0	0 ($\frac{2}{3}$) or 1 ($\frac{1}{3}$)
New state	$\|0001\rangle$	$\frac{1}{\sqrt{2}}\|0101\rangle + \frac{1}{\sqrt{2}}\|0001\rangle$ or $\|0110\rangle$

Superposition

Measurement

State	$\|0001\rangle$	$\frac{1}{\sqrt{3}}\|0110\rangle - \frac{1}{\sqrt{3}}\|0101\rangle + \frac{1}{\sqrt{3}}\|0001\rangle$
Measurement (third qubit)	0	0 ($\frac{2}{3}$) or 1 ($\frac{1}{3}$)
New state	$\|0001\rangle$	$\frac{1}{\sqrt{2}}\|0101\rangle + \frac{1}{\sqrt{2}}\|0001\rangle$ or $\|0110\rangle$

Hadamard Gate

$$H: \quad |0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Superposition

Measurement

State	$\|0001\rangle$	$\frac{1}{\sqrt{3}}\|0110\rangle - \frac{1}{\sqrt{3}}\|0101\rangle + \frac{1}{\sqrt{3}}\|0001\rangle$
Measurement (third qubit)	0	0 ($\frac{2}{3}$) or 1 ($\frac{1}{3}$)
New state	$\|0001\rangle$	$\frac{1}{\sqrt{2}}\|0101\rangle + \frac{1}{\sqrt{2}}\|0001\rangle$ or $\|0110\rangle$

Hadamard Gate

$$H: \quad |0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \mapsto \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle + \frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle = |0\rangle$$
$$|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Superposition

Measurement

State	$\|0001\rangle$	$\frac{1}{\sqrt{3}}\|0110\rangle - \frac{1}{\sqrt{3}}\|0101\rangle + \frac{1}{\sqrt{3}}\|0001\rangle$
Measurement (third qubit)	0	0 ($\frac{2}{3}$) or 1 ($\frac{1}{3}$)
New state	$\|0001\rangle$	$\frac{1}{\sqrt{2}}\|0101\rangle + \frac{1}{\sqrt{2}}\|0001\rangle$ or $\|0110\rangle$

Hadamard Gate

$$H: \quad |0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \mapsto \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle - \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle = |1\rangle$$

Hadamard Gate

$$H: \quad \begin{aligned} |0\rangle &\mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

On multiple qubits

$$|000\rangle \mapsto \frac{1}{\sqrt{8}}(\begin{aligned} &|000\rangle + |001\rangle + |010\rangle + |011\rangle + \\ &|100\rangle + |101\rangle + |110\rangle + |111\rangle) \end{aligned}$$

Hadamard Gate

$$
\begin{aligned}
H: \quad |0\rangle &\mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
|1\rangle &\mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
\end{aligned}
$$

On multiple qubits

$$
\begin{aligned}
|000\rangle \mapsto \frac{1}{\sqrt{8}}(& |000\rangle + |001\rangle + |010\rangle + |011\rangle + \\
& |100\rangle + |101\rangle + |110\rangle + |111\rangle) \\
|011\rangle \mapsto \frac{1}{\sqrt{8}}(& |000\rangle - |001\rangle - |010\rangle + |011\rangle + \\
& |100\rangle - |101\rangle - |110\rangle + |111\rangle)
\end{aligned}
$$

Hadamard Gate

$$\begin{aligned} H: \quad |0\rangle &\mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

On multiple qubits

$$\begin{aligned} |000\rangle \mapsto \frac{1}{\sqrt{8}}(& |000\rangle + |001\rangle + |010\rangle + |011\rangle + \\ & |100\rangle + |101\rangle + |110\rangle + |111\rangle) \\ |011\rangle \mapsto \frac{1}{\sqrt{8}}(& |000\rangle - |001\rangle - |010\rangle + |011\rangle + \\ & |100\rangle - |101\rangle - |110\rangle + |111\rangle) \end{aligned}$$

Compact form

$$H: |x\rangle \mapsto \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle$$

Simon's algorithm

Simon's problem

- $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$
- $s \in \mathbb{Z}_2^n$
- $\forall x, y, f(x \oplus y) = f(x) \Leftrightarrow x \oplus y \in \{0, s\}$
- f hides the period s
- Goal : find s, given oracle access to f.

Classical resolution

Seek for a collision, in $\Omega\left(2^{n/2}\right)$ samples.

Simon's algorithm

Quantum circuit

- *Start from* $|0\rangle\,|0\rangle$

Simon's algorithm

Quantum circuit

- Start from $|0\rangle |0\rangle$ $H|x\rangle \rightarrow \sum_y (-1)^{x \cdot y} |y\rangle$
- *Apply H, which gives* $\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle$

Simon's algorithm

Quantum circuit

- Start from $|0\rangle\,|0\rangle$ $\quad H|x\rangle \to \sum_y (-1)^{x\cdot y}|y\rangle \qquad O_f|x\rangle\,|0\rangle \to |x\rangle\,|f(x)\rangle$
- Apply H, which gives $\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle\,|0\rangle$
- *Apply O_f, which gives* $\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle\,|f(x)\rangle$

Simon's algorithm

Quantum circuit

- Start from $|0\rangle |0\rangle$ $\quad H|x\rangle \to \sum_y (-1)^{x\cdot y}|y\rangle \qquad O_f|x\rangle|0\rangle \to |x\rangle|f(x)\rangle$
- Apply H, which gives $\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle$
- Apply O_f, which gives $\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$
- *Measure the second register : we get $f(x_0)$ and project the first register to* $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus s\rangle)$

Simon's algorithm

Quantum circuit

- Start from $|0\rangle |0\rangle$ $\quad H|x\rangle \to \sum_y (-1)^{x\cdot y}|y\rangle \qquad O_f|x\rangle|0\rangle \to |x\rangle|f(x)\rangle$
- Apply H, which gives $\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle$
- Apply O_f, which gives $\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$
- Measure the second register : we get $f(x_0)$ and project the first register to $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus s\rangle)$
- *Reapply H to get* $\frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} (-1)^{x_0\cdot y}|y\rangle + (-1)^{(x_0\oplus s)\cdot y}|y\rangle$

Simon's algorithm

Quantum circuit

- Start from $|0\rangle|0\rangle$ $\quad H|x\rangle \to \sum_y (-1)^{x\cdot y}|y\rangle \qquad O_f|x\rangle|0\rangle \to |x\rangle|f(x)\rangle$
- Apply H, which gives $\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle|0\rangle$
- Apply O_f, which gives $\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle$
- Measure the second register : we get $f(x_0)$ and project the first register to $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus s\rangle)$
- Reapply H to get $\frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}(-1)^{x_0\cdot y}|y\rangle + (-1)^{(x_0\oplus s)\cdot y}|y\rangle$
- *The state is* $\frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}(-1)^{x_0\cdot y}(1+(-1)^{s\cdot y})|y\rangle$

We measure a value y_0 such that $1+(-1)^{s\cdot y_0} \neq 0 \Rightarrow y_0 \cdot s = 0$.

Simon's algorithm [Simon94]

Full algorithm

- Retrieve enough y_i with $y_i \cdot s = 0$.
- Solve the system to determine s.
- n equations are enough.
- $\mathcal{O}(n)$ vs $\mathcal{O}(2^{n/2})$

Generalisations

- Random periodic functions ($1.2n$) — Wider applications
- Functions that change at each query — No nonce reuse

Generalisation : Case of multiple periods

What if $f(x) = f(x \oplus s_1) = f(x \oplus s_2) (= f(x \oplus s_1 \oplus s_2))$?

- We'll have $y_i \cdot s_1 = 0$ and $y_i \cdot s_2 = 0$ (and $y_i \cdot (s_1 \oplus s_2) = 0$).
- The equation system we get defines $\langle s_1, s_2 \rangle$.
- We then need to distinguish s_1, s_2 and $s_1 \oplus s_2$.

Actually applicable to AEZ!

Allows to retrieve 2 or 3 subkeys at once.

Quantum attack on AEZ

Periodic functions for AEZv5

Period	Function
$6I$	$\text{Encrypt}(K, (\tau, N, (x, A, B, C, D, E, F, G, x), \epsilon)$
$3J$	$\text{Encrypt}(K, (\tau, N, x, x), \epsilon)$
$3L$	$\text{Encrypt}(K, (\tau, N, (x, x)), \epsilon)$
$\langle 3J, 3L \rangle$	$\text{Encrypt}(K, (\tau, N, (x, x), (x, x)), \epsilon)$

Cost

Version	Type	Classical cost	Quantum cost
AEZv4	Key recovery	$2^{66.5}$	$2^{11.4}$
AEZv5	Key recovery	2^{68}	$2^{11.1}$
AEZ10	Universal forgery	$2^{67.3}$	$2^{9.6}$

Quantum attack on AEZ

- See the collision analysis [CG16] as (multiple) period finding.
- Perfect use case for Simon's algorithm.
- Much better than quadratic quantum gap.

Classical analysis $\Rightarrow$ Quantum attack

Conclusion

A very efficient attack

Quantum (multiple) period finding can be applied on real-world symmetric primitives.

Is AEZ v4.1 Sufficiently Resilient Against Key-Recovery Attacks? (FSE17)

No (in this model).

Towards AEZv6?

Small changes in the algorithm seem to prevent the attack.