Caesar Candidate CMCC

Jonathan Trostle, Ph.D

CMCC Goals

- Compactness (minimize bits on the wire) in order to maximize energy efficiency for constrained environments
- Provable security
- Applicable to short plaintexts (including lengths less than cipher block length)
- CCA2 security without an authentication tag for constrained protocol scenarios and to gain upper layer protocol checks as authentication bits
- Nonce misuse resistance

Problem Space/Applications

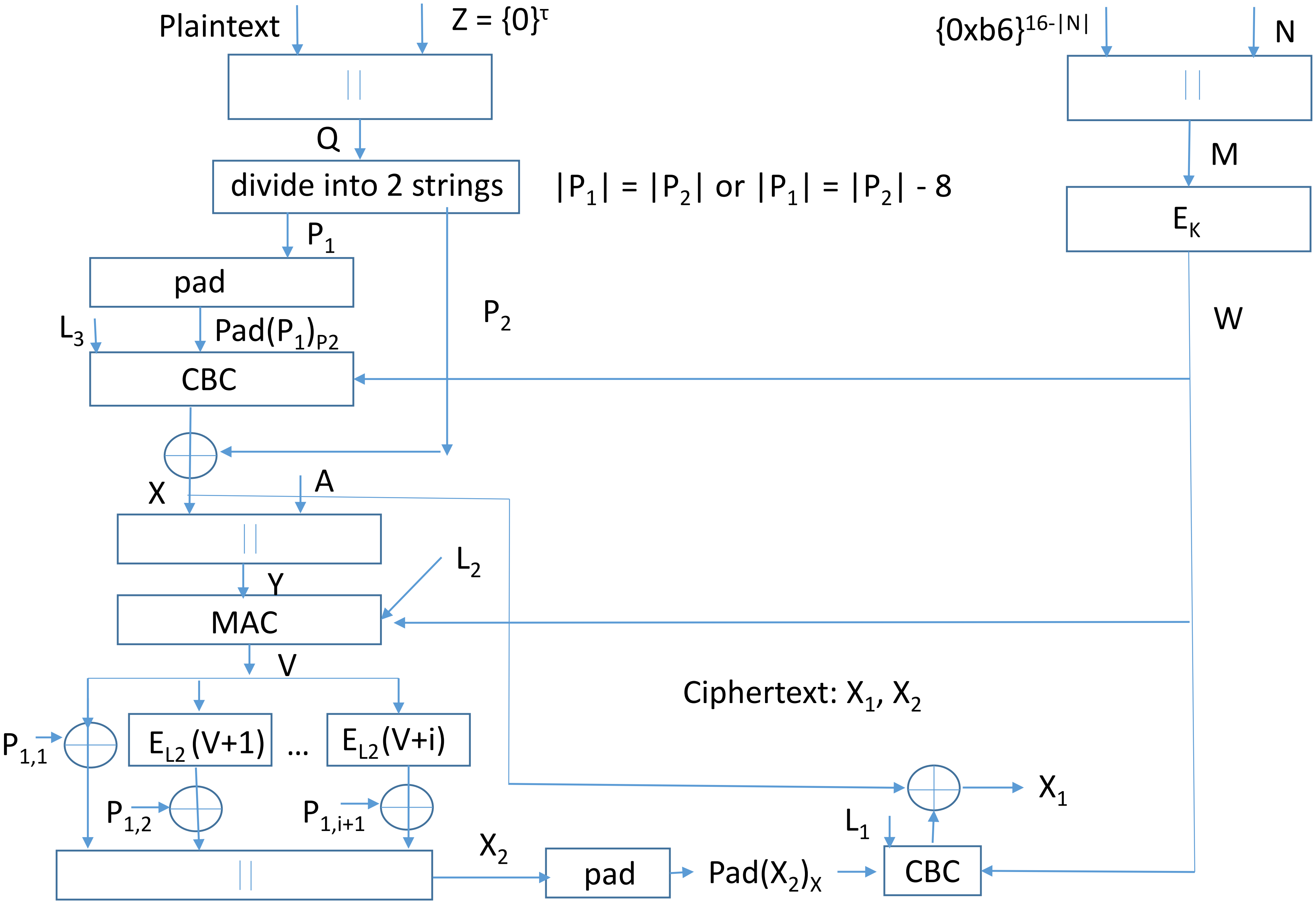
- Targeted at environments with short messages due to energy constraints
  - Energy usage proportional to message length
  - Reducing ciphertext expansion more important than CPU processing overhead
  - Large numbers of queries likely to be either impossible or highly anomalous on these constrained low bandwidth networks
- Wireless sensor networks
- Internet of Things (Rene Struik presentation)
- VoIP

Quick Description of CMCC Stateless Version

- Inputs plaintext P and nonce N and divide P into two equal size strings P1 and P2: P = P1 | P2.
- Block cipher encrypt N after prepending a constant to get M
- CBC encrypt P1 and XOR P2 to get X (M is IV): X = CBC(M,P1) XOR P2
- V = MAC (M|X|A); use V as counter mode IV and encrypt P1
- X1 = CBC(M, X2) XOR X
- Ciphertext is X1, X2
- AEAD: Replace P with P|Z where Z is a string of zero bits

Intuition for Security

- If there are no W|X|A collisions, then since MAC is PRF, MAC(W|X|A) is pseudorandom and counter mode hides P1
- X2 pseudorandom so CBC(M,X2) hides X
- Decryption queries: if there are no P1 collisions then P2 remains hidden
- Decryption queries can be partially defended via the authentication tag



Plaintext
Z = {0}τ
||
Q
divide into 2 strings
|P1| = |P2| or |P1| = |P2| - 8
P1
pad
L3
Pad(P1)P2
P2
CBC
X
A
||
Y
L2
MAC
V
P1,1
EL2(V+1)
...
EL2(V+i)
P1,2
P1,i+1
||
X2
pad
Pad(X2)X
L1
CBC
X1
Ciphertext: X1, X2
{0xb6}16-|N|
N
||
M
EK
W

Cryptanalysis

- Guy Barwell from University of Bristol discovered simple attacks based on colliding X values for plaintexts of different lengths
- Padding scheme was inadequate and is now revised
- Using CMAC padding scheme and padding collision bound incorporated into proof

Security Bounds

- Beta is the minimum of the block length and half the length of the plaintext plus the length of the authentication tag for the challenge ciphertext
- Privacy bound dominated by q/Beta if message numbers not reused (CCA2 security), zero length authentication tag
- Bound dominated by $1/(2^T \text{Beta})$ given authentication tag with T bits if invalid queries terminate session and message numbers not reused
- $q/(2^T \text{Beta})$ if the authentication tag is computed using a keyed MAC algorithm but invalid queries are allowed, no reuse of message no's
- $q(q-1)/\text{Beta} + 1/2^T$ for misuse resistance (2^T -> 2^{2T} for keyed MAC)

Tweaks

- Key K for block cipher invocation on nonce to obtain message number plus separate keys (4) for each of the two CBC, MAC and CTR operations
  - Propose using same key L2 for MAC and CTR
- Can replace zero bit string Z with a keyed MAC over plaintext to get a stronger security bound
- Investigate underlying primitives other than AES (e.g., universal hashing, etc.)

Ciphertext Expansion

- Authentication tag can be of any length
- CCA security of CMCC implies authentication tag can be shorter than some existing mode authentication tag since upper layer protocol checks will most likely fail when ciphertext is modified
- Stateless scheme nonce size determines maximum number of messages that can be sent without cycling on message numbers for given key
- Stateful version of CMCC (not submitted to Caesar) allows different trade-off – constraint is bound on reordering for encryption and decryption

Advantages

- Simplicity (both design level and implementation level)
- Provable security (from standard prf assumption)
- CCA2 security with no authentication tag for scenarios where tag must be omitted
- Ciphertext modification results in plaintext randomization implies gain of upper layer protocol checks as additional authentication bits
- Energy efficiency (due to minimal expansion)
  - Most important performance metric for energy constrained wireless networks instead of CPU processing efficiency
- Nonce misuse resistance
- Full range of plaintext sizes including lengths less than cipher block length

Disadvantages

- Not online
- Not a one pass algorithm

Future Work

- Implement over other symmetric encryption algorithms, MAC algorithms (e.g. universal hashing)
- Optimized implementation
- Eprint paper: 2013/269