FAST PROTECTION OF H.264/AVC BY SELECTIVE ENCRYPTION OF CABAC

Zafar SHAHID, Marc CHAUMONT, William PUECH
(zafar.shahid@lirmm.fr)
LIRMM, UMR CNRS 5506, Université Montpellier II

Talk Outline

LIRMM

- ✓ Problem Statement
- ✓ CABAC
  - ✓ Block diagram
  - ✓ Binarization
- ✓ Proposed Approach
  - ✓ Proposed scheme in H.264/AVC
  - ✓ Proposed scheme for non-zero coefficients
  - ✓ Encryption process
- ✓ Results
  - ✓ Visual comparison of encrypted frames at different QPs
  - ✓ Foreman sequence encryption at different QPs
  - ✓ Nine benchmark video sequences results at same QP.
- ✓ Conclusions

LIRMM

Problem Statement

To perform selective encryption (SE) of CABAC for real-time protection of H.264/AVC bitstream.

Constraints:

- ✓ Same bitrate
- ✓ No increase in processing power
- ✓ Browseable bitstream

Our Approach

LIRMM

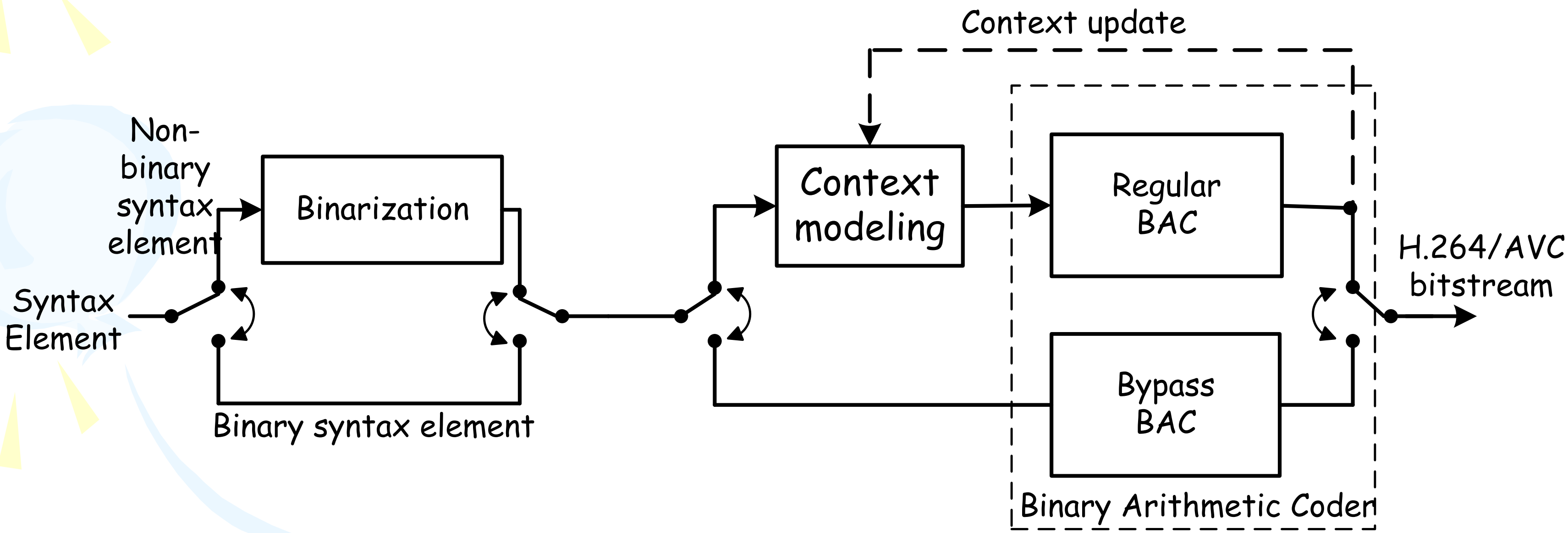
1. SE is performed in Context-based Adaptive Binary Arithmetic Coding (**CABAC**) module.
2. **Same bitrate** is achieved through scrambling of only equal length binarized code words.
3. Encrypted bitstream is **completely compliant** to H.264/AVC format. (ONLY MB data is encrypted.)

Talk Outline

LIRMM

- ✓ Problem Statement
- ✓ CABAC
  - ✓ Block diagram
  - ✓ Binarization
- ✓ Proposed Approach
  - ✓ Proposed scheme in H.264/AVC
  - ✓ Proposed scheme for non-zero coefficients
  - ✓ Encryption process
- ✓ Results
  - ✓ Visual comparison of encrypted frames at different QPs
  - ✓ Foreman sequence encryption at different QPs
  - ✓ Nine benchmark video sequences results at same QP.
- ✓ Conclusions

CABAC


Context update
Non-binary syntax element
Binarization
Context modeling
Regular BAC
H.264/AVC bitstream
Syntax Element
Bypass BAC
Binary syntax element
Binary Arithmetic Coder

CABAC

LIRMM

CABAC codes the input data in the following steps:

1. Binarization

   It is performed in one of the following ways:

   1. The unary code
   2. The truncated unary code
   3. The kth order Exp-Golomb code
   4. The fixed length code

2. Context modeling

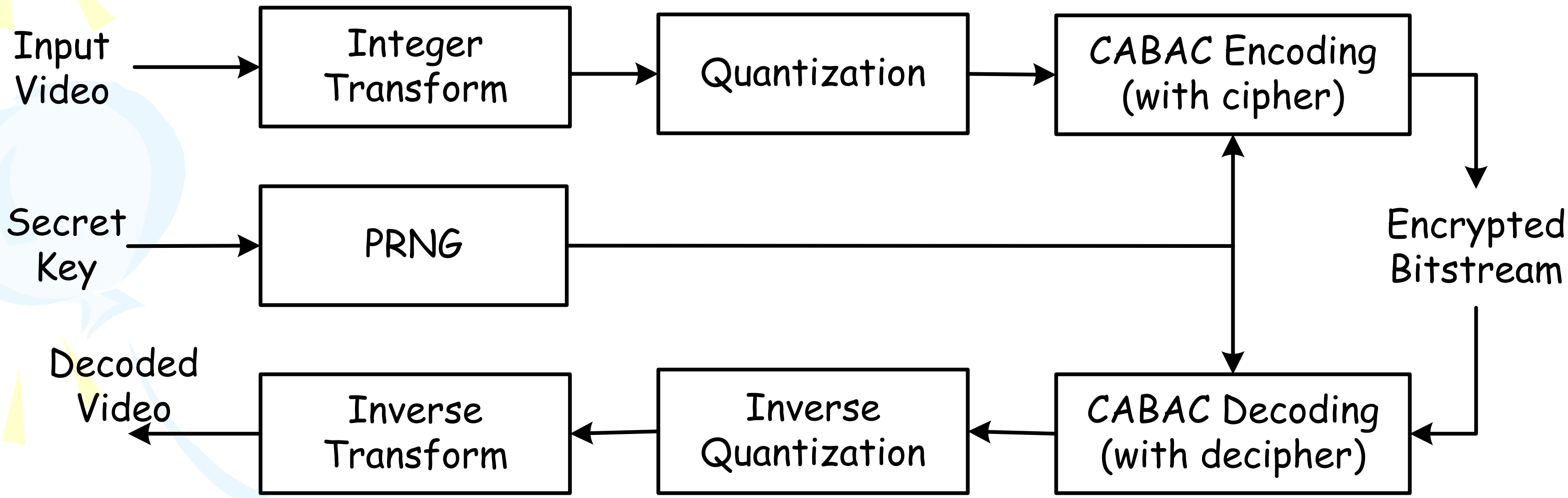
3. Binary Arithmetic Coding

Talk Outline

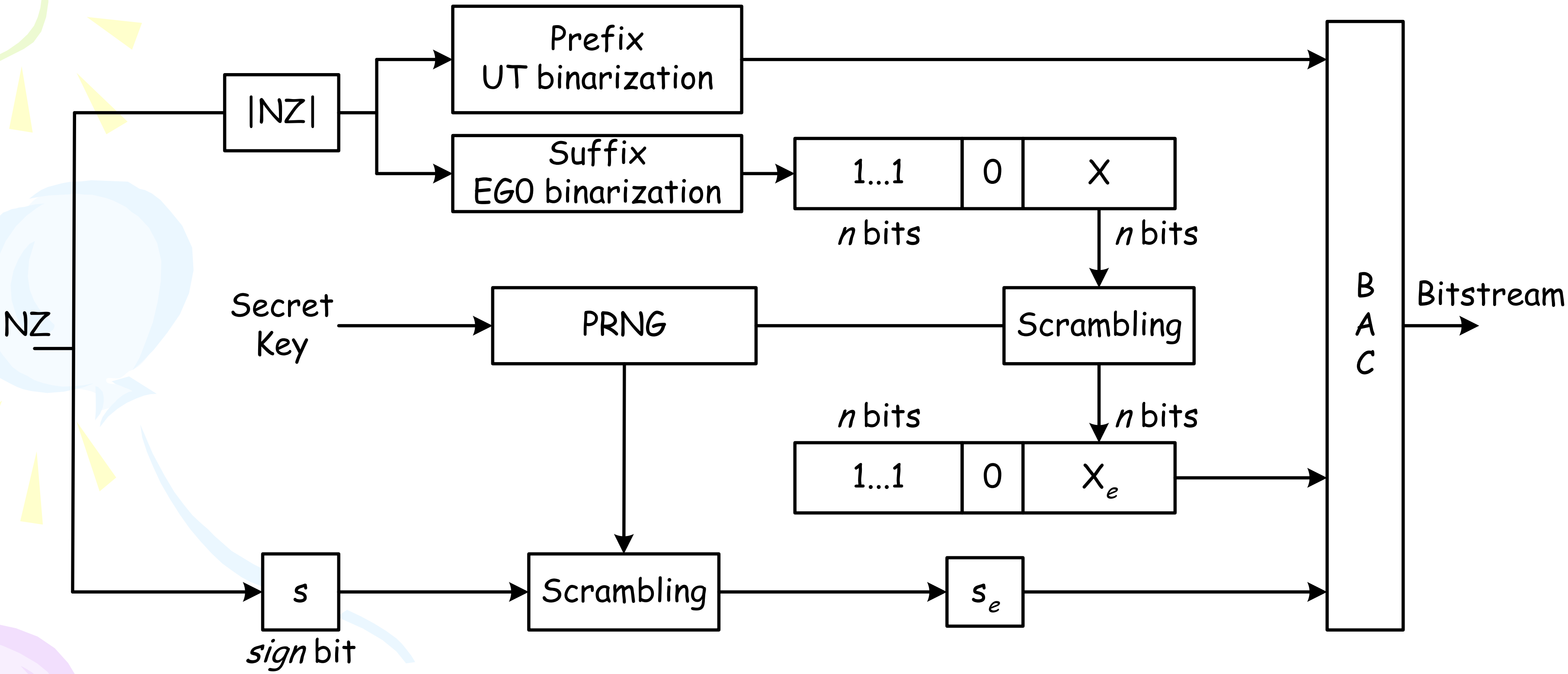
LIRMM

- ✓ Problem Statement
- ✓ CABAC
  - ✓ Block diagram
  - ✓ Binarization
- ✓ Proposed Approach
  - ✓ Proposed scheme in H.264/AVC
  - ✓ Proposed scheme for non-zero coefficients
  - ✓ Encryption process
- ✓ Results
  - ✓ Visual comparison of encrypted frames at different QPs
  - ✓ Foreman sequence encryption at different QPs
  - ✓ Nine benchmark video sequences results at same QP.
- ✓ Conclusions

Proposed Algorithms



Proposed Algorithms



Encryption Process

LIRMM

- NZs are scrambled with only those NZs whose EG0 (0th order Exp-Golomb code) codes have the same length.
- **For encryption process:**
- Let X be a suffix part of absolute level of NZ. It is encrypted with the encrypted coefficient y:
  - $y = (x + y) \bmod \log2(x + 1)$,
- Where
  - $y = rand() \bmod \log2(x + 1)$.
- **For decryption process:**
- For the decryption of NZs in H.264/AVC decoder:
  - $x = (y + \log2(n + 1) - y)) \bmod \log2(y + 1)$.

Talk Outline

LIRMM

- Problem Statement
- CABAC
  - Block diagram
  - Binarization
- Proposed Approach
  - Proposed scheme in H.264/AVC
  - Proposed scheme for non-zero coefficients
  - Encryption process
- **Results**
  - Visual comparison of encrypted frames at different QPs
  - Foreman sequence encryption at different QPs
  - Nine benchmark video sequences results at same QP.
- Conclusions

Results: Foreman 1st Frame at diff. QPs

QP = 18

QP = 24

QP = 30

QP = 36

Results – Foreman seq. at diff. QPs

LIRMM

QP	PSNR (Y) (dB)		PSNR (U) (dB)		PSNR (V) (dB)	
	Without SE	With SE	Without SE	With SE	Without SE	With SE
18	44.43	8.42	45.62	23.87	47.42	22.14
24	39.40	8.38	41.70	24.87	43.86	22.70
30	34.93	8.92	39.38	24.60	40.99	22.71
36	30.80	8.89	37.33	24.65	38.10	22.90

Results – Nine seq. at QP = 18

Seq.	PSNR (Y) (dB)		PSNR (U) (dB)		PSNR (V) (dB)	
	Without SE	With SE	Without SE	With SE	Without SE	With SE
bus	44.26	7.73	45.22	25.19	46.50	26.86
city	44.28	11.52	45.83	30.50	46.76	31.86
crew	44.81	9.39	45.81	23.80	45.66	19.90
football	44.59	11.46	45.70	15.79	45.98	23.10
foreman	44.43	8.42	45.62	23.87	47.42	22.14
harbour	44.10	9.48	45.60	23.82	46.63	31.20
ice	46.56	10.37	48.70	25.42	49.19	19.73
mobile	44.45	8.42	44.14	13.47	44.04	11.11
soccer	44.26	10.84	46.59	19.69	47.82	24.83

Talk Outline

LIRMM

- ✓ Problem Statement
- ✓ CABAC
  - ✓ Block diagram
  - ✓ Binarization
- ✓ Proposed Approach
  - ✓ Proposed scheme in H.264/AVC
  - ✓ Proposed scheme for non-zero coefficients
  - ✓ Encryption process
- ✓ Results
  - ✓ Visual comparison of encrypted frames at different QPs
  - ✓ Foreman sequence encryption at different QPs
  - ✓ Nine benchmark video sequences results at same QP.
- ✓ Conclusions

Conclusions

LIRMM

Encouraging results in the following contexts:

- ✓ Equally efficient algorithm over whole range of QP values.
- ✓ Real-time constraints successfully handled for:
  - ✓ Heterogeneous networks (exactly the same birate),
  - ✓ Handheld devices (minimal set of computational requirements),
  - ✓ Encrypted bitstream browsing (H.264/AVC compliant bitstream).
- ✓ The work can be extended for:
  - ✓ Protection of ROI,
  - ✓ Medical image transmission,
  - ✓ Protection of P and B frames in H.264/AVC.