Intel® Integrated Performance Primitives (Intel® IPP)
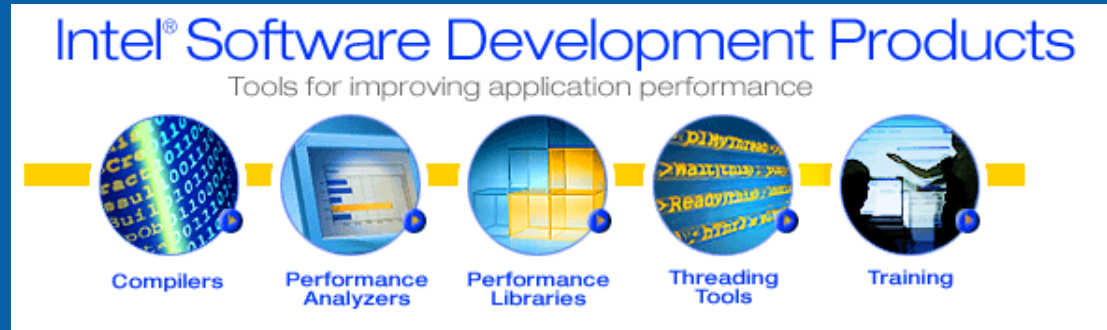
Shinn Lee
IPP Chief Architect
OpenCV Syposium, Beijing, June 2007

Intel® Software Development Products
Tools for improving application performance

Compilers   Performance Analyzers   Performance Libraries   Threading Tools   Training

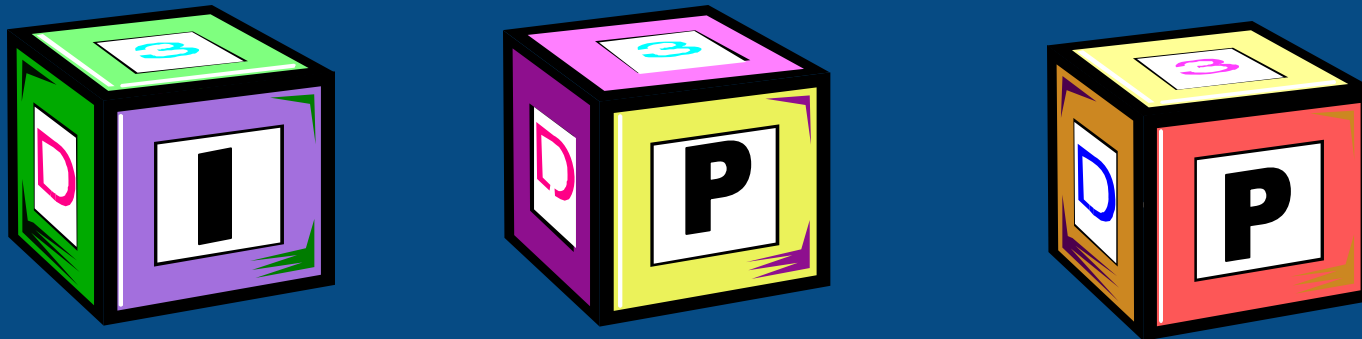**Performance**   **Compatibility**   **Support**

www.intel.com/software/products

Intel Confidential

What Is A Primitive?

- A **low level** building block that
  - Abstracts low-level implementation details
  - Performs a single operation
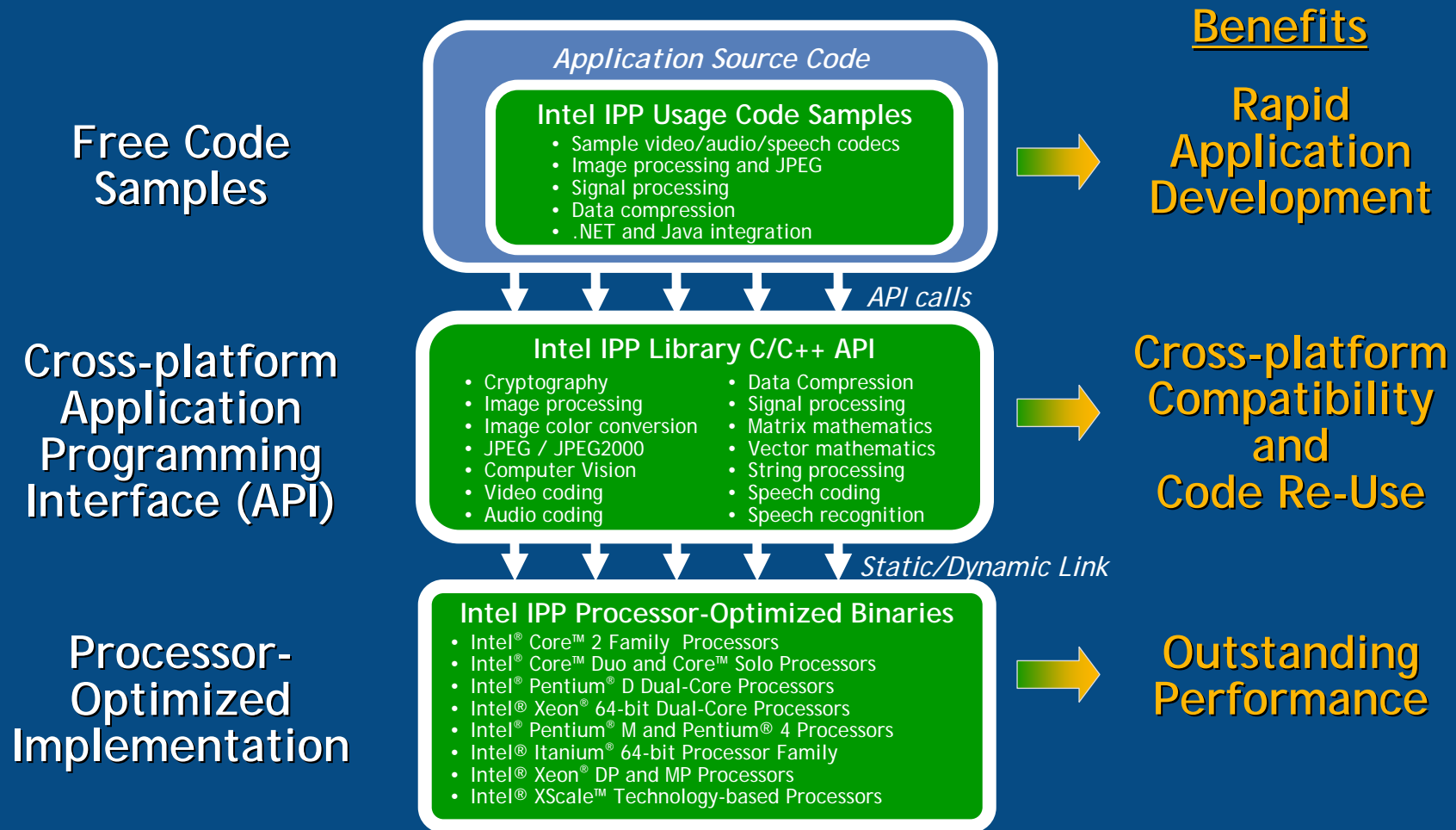 - Is a component piece of a larger solution

Intel Confidential

http://www.intel.com/software/products

What Are IPP ?

- Huge collection of useful multimedia functions
  - Mathematics, signal, speech, audio, video, image, graphics

- Low-level and simplex

- Highly-optimized, processor-specific code

- Common across multiple platforms
  - desktop, and server processors
  - Windows*, Linux operation systems

- Widely used, well-received product

Intel Confidential

http://www.intel.com/software/products

Intel® Integrated Performance Primitives (Intel® IPP) — Overview and Benefits

Free Code Samples

Application Source Code

Intel IPP Usage Code Samples
- Sample video/audio/speech codecs
- Image processing and JPEG
- Signal processing
- Data compression
- .NET and Java integration

API calls

Rapid Application Development

Cross-platform Application Programming Interface (API)

Intel IPP Library C/C++ API
- Cryptography
- Image processing
- Image color conversion
- JPEG / JPEG2000
- Computer Vision
- Video coding
- Audio coding
- Data Compression
- Signal processing
- Matrix mathematics
- Vector mathematics
- String processing
- Speech coding
- Speech recognition

Static/Dynamic Link

Cross-platform Compatibility and Code Re-Use

Processor-Optimized Implementation

Intel IPP Processor-Optimized Binaries
- Intel® Core™ 2 Family Processors
- Intel® Core™ Duo and Core™ Solo Processors
- Intel® Pentium® D Dual-Core Processors
- Intel® Xeon® 64-bit Dual-Core Processors
- Intel® Pentium® M and Pentium® 4 Processors
- Intel® Itanium® 64-bit Processor Family
- Intel® Xeon® DP and MP Processors
- Intel® XScale™ Technology-based Processors

Outstanding Performance

Intel Confidential

http://www.intel.com/software/products

The 14 15 Domains in IPP

1. Static Pictures
- Image Processing
- Computer Vision
- JPEG (Image coding)
- Ray-Tracing/Rendering*

2. Motion Pictures
- Video Coding
- Color Conversion

3. Sound and Speech
- Audio Coding
- Speech Coding
- Speech Recognition

4. Computer Data
- Data Compression
- Cryptography
- Text string processing

5. Mathematics
- Digital Signal Processing
- Small matrices
- Vectors

* new in Intel IPP 5.2 (Q2-2007)

Intel Confidential

(intel) Software

http://www.intel.com/software/products

(intel)

IPP 5.x Domains and Functions

	Domain	IA	IXP	
Image Processing	**ippi**	**2570**	**1574**	
Signal Processing	**ipps**	**1865**	**783**	
Speech Recognition	**ippsr**	**618**	**618**	
Computer Vision	**ippcv**	**417**	**417**	
Color Conversion	**ippcc**	**410**	**410**	
Cryptography	**ippcp**	**307**	**307**	
Speech Coding	**ippsc**	**297**	**247**	
Video Coding	**ippvc**	**219**	**219**	
Image Coding	**ippj**	**201**	**201**	
Audio Coding	**ippac**	**152**	**152**	
Data Compression	**ippdc**	**73**	**73**	
Char Processing	**ippch**	**72**	**72**	
Small Matrix	**ippm**	**669**	**0**	
Vector Math	**ippvm**	**136**	**0**	
Totals		**8006**	**5082**	

(intel)
Software

Intel, Itanium, Pentium, and the Intel logo are trademarks or registered trademarks of Intel
Corporation or its subsidiaries in the United States or other countries.
http://www.intel.com/software/products

(intel)

Intel IPP:
Codec and Data Processing Standards Support

- Video Codecs
  - H.264
  - H.263
  - H.261
  - MPEG-4
  - MPEG-2
  - Motion JPEG
  - DV
- Audio Codecs
  - MP3
  - AAC
  - AC3
- Image Codecs
  - JPEG
  - JPEG2000

- Speech Codecs
  - AMR-WB
  - G.711 / I / II
  - G.722.1 G.722.2 (GSM-AMR)
  - G.723.1 / A
  - G.726 / A
  - G.728 G/I/H
  - G.729, G.729A, G.729D, G.729E, G.729I
  - GSM-FIR
  - GSM 06.90-06.94
  - GSM 06.10-06.12
  - GSM 06.31-06.32
- Echo Cancellation
  - G.168-2000
  - G.167
- Speech Recognition
  - Aurora
  - Advanced Aurora
  - Gaussian Mixture

- Data Compression
  - Huffman encoding/decoding
  - RLE encoding/decoding
  - MoveToFront (MTF)
  - Burrows-Wheeler Transformations (BWT)
  - General Interval Transform (GIT)
  - Lempel-Ziv-Storer-Szymanski (LZSS) functions
- Cryptography
  - Rijndael, DAARijndael
  - DES, DAA-DES
  - Triple DES, DAA-TDES
  - Twofish, DAA-Twofish
  - Blowfish, DAABlowfish
  - SHA1, SHA256/384/512, HMAC-SHA1
  - MD5, HMAC-MD5
  - Digital Signature Algorithm (DSA)

Intel IPP helps you Benefit from New Standards

9

Software

Intel Confidential

http://www.intel.com/software/products

(intel)

UMC: IPP based codec

- What is it?
  - A set of unified C++ interface for media building blocks:
  - Designed for portability, allow cross platform (uArch, OS) support
- Benefits of using UMC
  - Simplifies media application development by providing consistent interface to all codecs
  - Simplifies adding new codec support
  - Simplifies porting application to new platform and easy to integrate with DirectShow, GStreamer
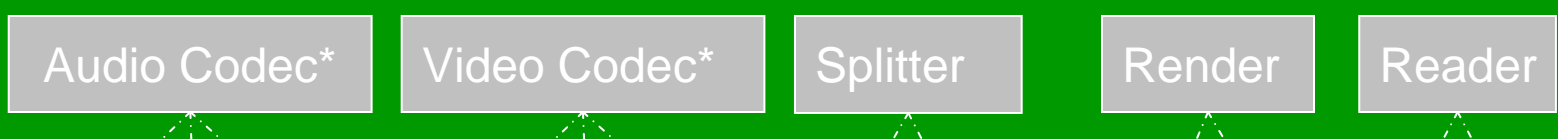- Introduced as sample in 5.0
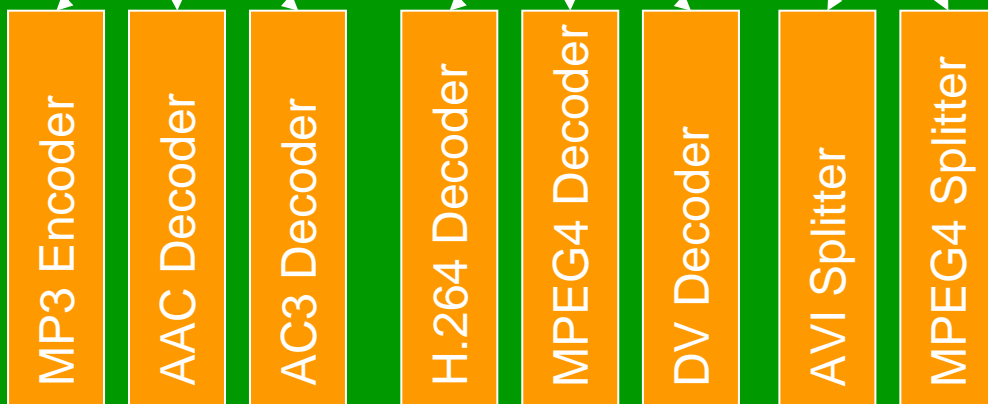 - Combine all media samples into one package

Intel Confidential

(intel)
Software

http://www.intel.com/software/products

(intel)

UMC Architecture

Application Layer

Decoding/encoding/transcoding applications, DShow filters, plug-ins

UMC Base Classes (Abstract Base Classes)

Audio Codec* Video Codec* Splitter Render Reader

UMC Derivative Classes (Codec's)   **OS-Dependent Renders**

MP3 Encoder AAC Decoder AC3 Decoder H.264 Decoder MPEG4 Decoder DV Decoder AVI Splitter MPEG4 Splitter DirectX Render SDL Render File Reader Socket Reader
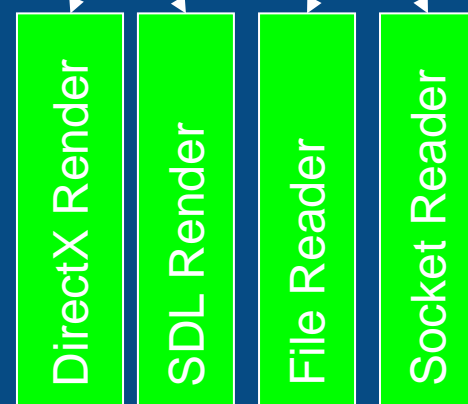
VM Library – OS Abstraction Layer

IPP Libraries

- illustration purpose only, more codec support in 50 gold.

Intel Confidential

(intel) Software

(intel)

http://www.intel.com/software/products

Codec Support in OS/Platform

Codec components	IA-32		Intel® EM64T		Itanium® processors		Intel® IXP 4XX Product Line of Network Processors		
	L	W	L	W	L	W	L(LE)	L(BE)	W
AAC audio decoder (integer based)	●	●	●	●	●	●	●	●	●
AAC audio decoder (floating point based)	●	●	●	●	●	●	N/A	N/A	N/A
AC3 audio decoder	●	●	●	●	●	●	N/A	N/A	N/A
MP3 audio decoder (integer based)	●	●	●	●	●	●	●	●	●
MP3 audio decoder (float point based)	●	●	●	●	●	●	N/A	N/A	N/A
AAC audio encoder (integer based)	●	●	●	●	●	●	●	●	●
AAC audio encoder (floating point based)	●	●	●	●	●	●	N/A	N/A	N/A
MP3 audio encoder (integer based)	●	●	●	●	●	●	●	●	●
MP3 audio encoder (floating point based)	●	●	●	●	●	●	N/A	N/A	N/A
…….More…………………..									

"●" - Validated as of IPP 5.0
"●" - Not supported yet
"N/A"- Not available due to absence of corresponding APIs for this platform
L – Linux*
W – Windows*

Intel Confidential

intel Software

http://www.intel.com/software/products

(intel)

Continued....

Codec components	IA-32		Intel® EM64T		Itanium® processors		Intel® IXP 4XX Product Line of Network Processors		
	L	W	L	W	L	W	L(LE)	L(BE)	W
....									
DV video decoder	●	●	●	●	●	●	●	●	●
MPEG 2 video decoder	●	●	●	●	●	●	●	●	●
MPEG 4 video decoder	●	●	●	●	●	●	●	●	●
MJPEG video decoder	●	●	●	●	●	●	●	●	●
H.261 video decoder	●	●	●	●	●	●	●	●	●
H.263 video decoder	●	●	●	●	●	●	●	●	●
H.264 video decoder	●	●	●	●	●	●	●	●	●
MPEG-2 video encoder	●	●	●	●	●	●	●	●	●
MPEG 4 video encoder	●	●	●	●	●	●	●	●	●
H.264 video encoder	●	●	●	●	●	●	●	●	●
H.261 video encoder	●	●	●	●	●	●	●	●	●
H.263 video encoder	●	●	●	●	●	●	●	●	●
AVI splitter	●	●	●	●	●	●	●	●	●
MP4 splitter	●	●	●	●	●	●	●	●	●
MPEG-2 PS/TS splitter	●	●	●	●	●	●	●	●	●

Start integrating UMC-based media codec for your development!

20

Intel Confidential

http://www.intel.com/software/products

Intel® IPP Crypto is...

- Variety of crypto functions – block ciphers, hash-functions, public-key cryptography

Symmetric ciphers	DES, 3DES, Blowfish, TwoFish, Rijndael, RC5
Stream ciphers	RC4
Hashing	SHA1, SHA256, SHA224, SHA512, SHA384, MD5, HMAC, DAA
Asymmetric ciphers and Schemes	RSA, RSAES-OAEP
Key agreement	DLSVDP-DH, ECSVDP-DH, ECSVDP-DHC
Digital Signature Generation/Verification and Schemes	DLSP-DSA, DLVP-SSA, ECSP-DSA, ECVP-DSA, ECSP-NR, ECVP-NR, RSASSA-PSS
Miscellaneous	Big Number, Finite Fields and Polynomial Arithmetic

397 crypto functions in IPP 5.2 gold

Intel Confidential

http://www.intel.com/software/products

(intel)
Software

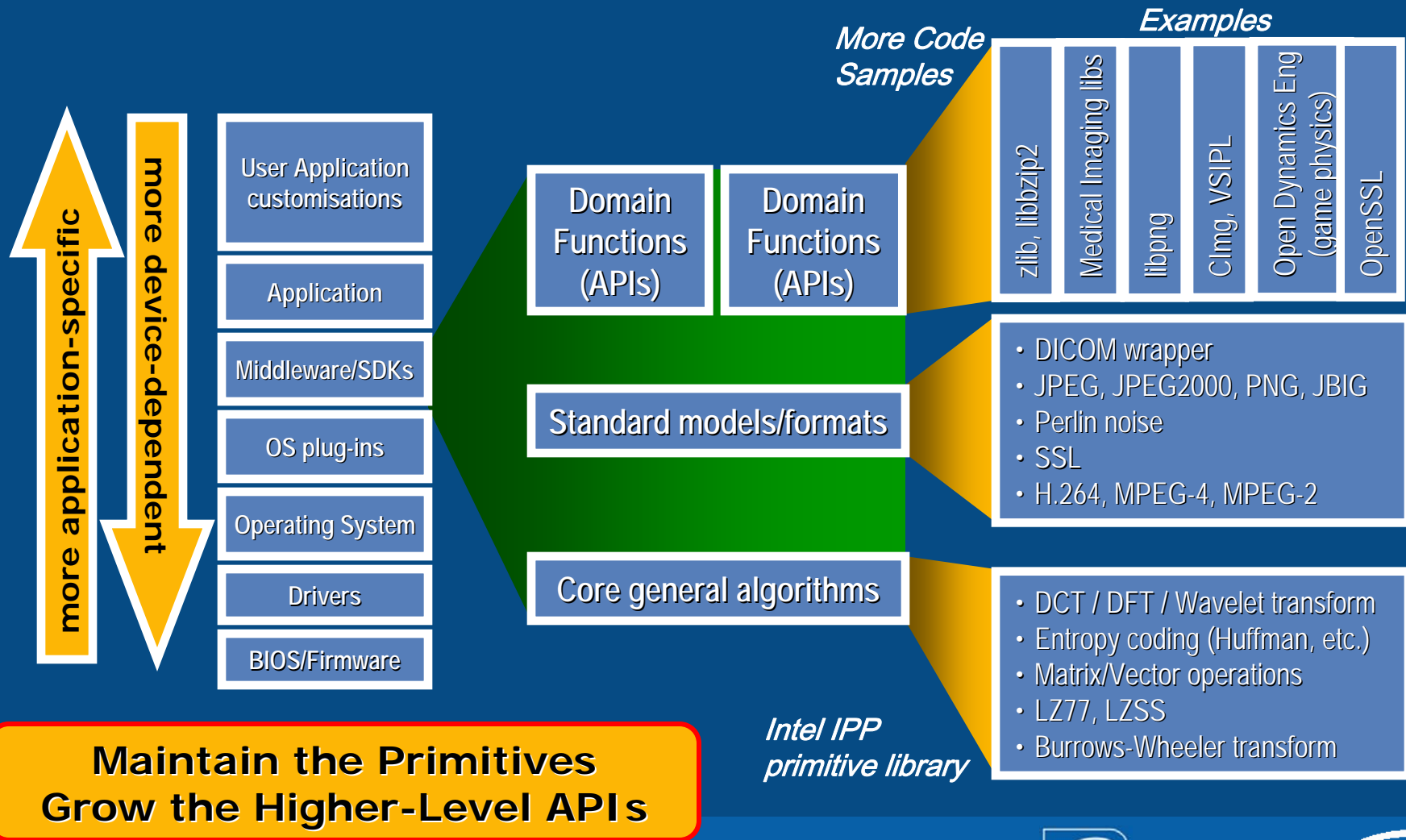(intel)

Threading Optimization in IPP Crypto Library

- Optimized for Intel® IA-32, Intel® x64, Itanium®-based platform and Intel XScale microarchitectures;
- Special tuning for multi-core Intel CPUs has been done wherever is possible

algorithm/function	single-thread	multi-thread (2x2Duo 3GHz)
Decrypt Rijndael-128-CBC	~20 cpe	~7 cpe
Decrypt Rijndael-192-CBC	~26 cpe	~7.5 cpe
Decrypt Rijndael-256-CBC	~28 cpe	~8 cpe
Decrypt RSA-1024	1380 op/s	2380 op/s
Decrypt RSA-2048	190 op/s	375 op/s
Decrypt RSA-4096	27 op/s	54 op/s

98 of 397 crypto functions are threaded in IPP

Intel Confidential

(intel)
Software

(intel)

http://www.intel.com/software/products

Directions for Future Development

More Code Samples

Examples

| zlib, libbzip2 | Medical Imaging libs | libpng | Cimg, VSIPL | Open Dynamics Eng (game physics) | OpenSSL |

Domain Functions (APIs) | **Domain Functions (APIs)**

- DICOM wrapper
- JPEG, JPEG2000, PNG, JBIG
- Perlin noise
- SSL
- H.264, MPEG-4, MPEG-2

Standard models/formats

Core general algorithms

- DCT / DFT / Wavelet transform
- Entropy coding (Huffman, etc.)
- Matrix/Vector operations
- LZ77, LZSS
- Burrows-Wheeler transform

Intel IPP primitive library

more application-specific

more device-dependent

- User Application customisations
- Application
- Middleware/SDKs
- OS plug-ins
- Operating System
- Drivers
- BIOS/Firmware

**Maintain the Primitives
Grow the Higher-Level APIs**

Intel Confidential

http://www.intel.com/software/products

intel Software

(intel)

Higher-Level APIs

Examples in the Market Today:
- Data Compression:
  - zlib, libbzip2
- Medical/Document Imaging:
  - Pegasus Imaging
  - LeadTools
  - Accusoft
  - Snowbound Software
  - libPNG
- Encrypted communications:
  - OpenSSL
- Computer Vision
  - OpenCV
- Signal Processing
  - VSIPL++

Proposed Strategy:

- Use Code Samples to enter higher-level API market

- "Promote" code samples into binary-only, new libraries
  - higher performance than code samples

Question:
- Will ISVs object to not having source code?

Intel Confidential

(intel)
Software

http://www.intel.com/software/products

(intel)

Summary

- IPP is a broad library for many market segments
  - 15 domains total, covering ~9000 functions
  - Opportunities in compressing/uncompressing data:
    - "human data": images, video, audio, speech
    - "computer data": lossless compression, encryption, text
- IPP 5.2 Gold released now
  - push on multi-core and 64-bit Core2
  - push on Enterprise data compression/transmission
  - push on Healthcare imaging
- Future IPP versions
  - shift to higher-level APIs

Intel Confidential

intel Software

http://www.intel.com/software/products

intel

Reference and Contacts:

- **External:**

  - **Intel® IPP Product Web Site**
    (releases info, Features, Samples, performance data, licensing, etc)

  - **Intel® IPP Support Web Site**
    (FAQs, Top critical issues, etc)

  - **Intel® Premier Support**
    (Technical Support, software update, etc)

  - **Intel® IPP Forum**
    (Technical discussion with other developers)

- Contacts:
  - Technical Consulting Engineers:
    Ying Hu
  - Business Development Manager
    Wei Lin
  - Product Marketing Manager
    Siang-Chun The

- **H264 doc:**

  - ITU-T Standard

  - H264 short overview

Intel Confidential

http://www.intel.com/software/products

intel Software

intel