
Secure FPGAs

Embedded World 2008

Lattice Semiconductor

Harald Werner

Area Technical Manager Central Europe

Agenda

- ◆ **Security Overview**

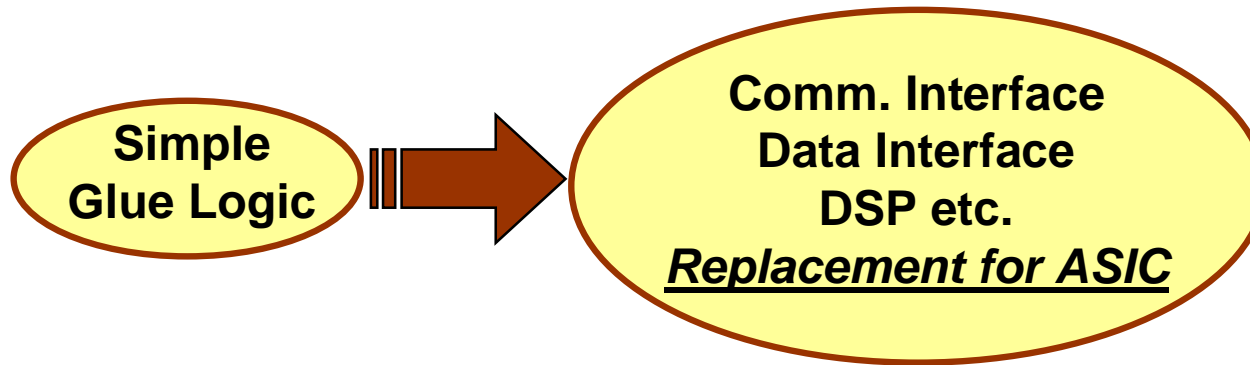
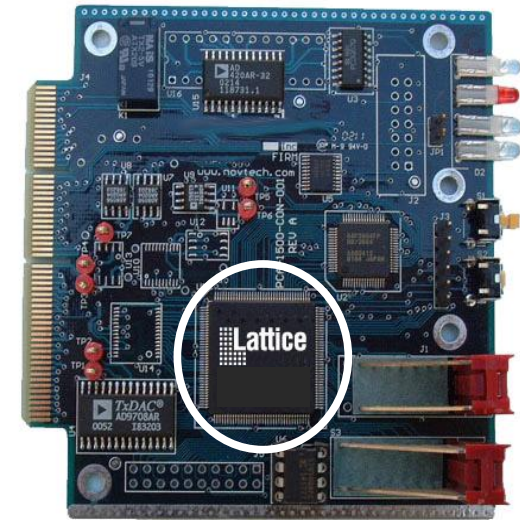
- ◆ **LatticeECP2S Device Security**

- ◆ **LatticeXP2 Device Security**

- ◆ **Summary**

FPGAs At The Heart of System

- ❑ As the FPGA performance capability increases and gets more cost-effective, FPGAs are becoming the logic device of choice for many applications.
- ❑ FPGAs continue to grow in density and capability, enabling users to implement more complex and valuable designs as the center engine of the board.



This shift has created the need for **Secure Programmable Logic Solutions** to protect expensive and proprietary intellectual property.

Common Security Concerns

◆ Reverse Engineering

- Analyzing an existing system to identify its components and their interrelationships. This information is typically used by competitors to improve their own designs or products.

◆ Cloning

- Making an exact copy of the system without having to determine the exact implementation details.

◆ Overbuilding

- A contract manufacturer building more than the requested number of systems, and selling the extra systems in the open market. All profits go directly to the contract manufacturer.

◆ Theft of Service

- An unauthorized individual reprograms electronic components running in a critical part of a network / telecom system in order to change the operation of the system for financial gain.

Agenda

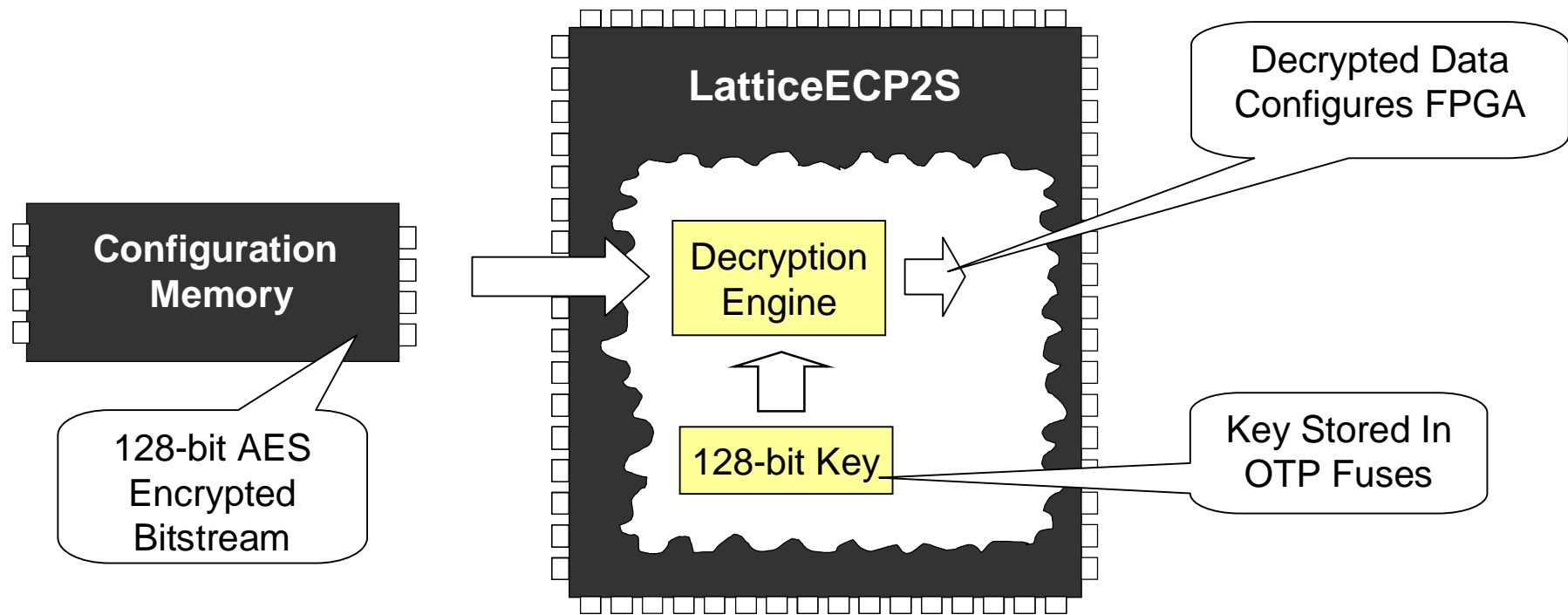
- ◆ Security Overview

- ◆ LatticeECP2S Device Security

- ◆ LatticeXP2 Device Security

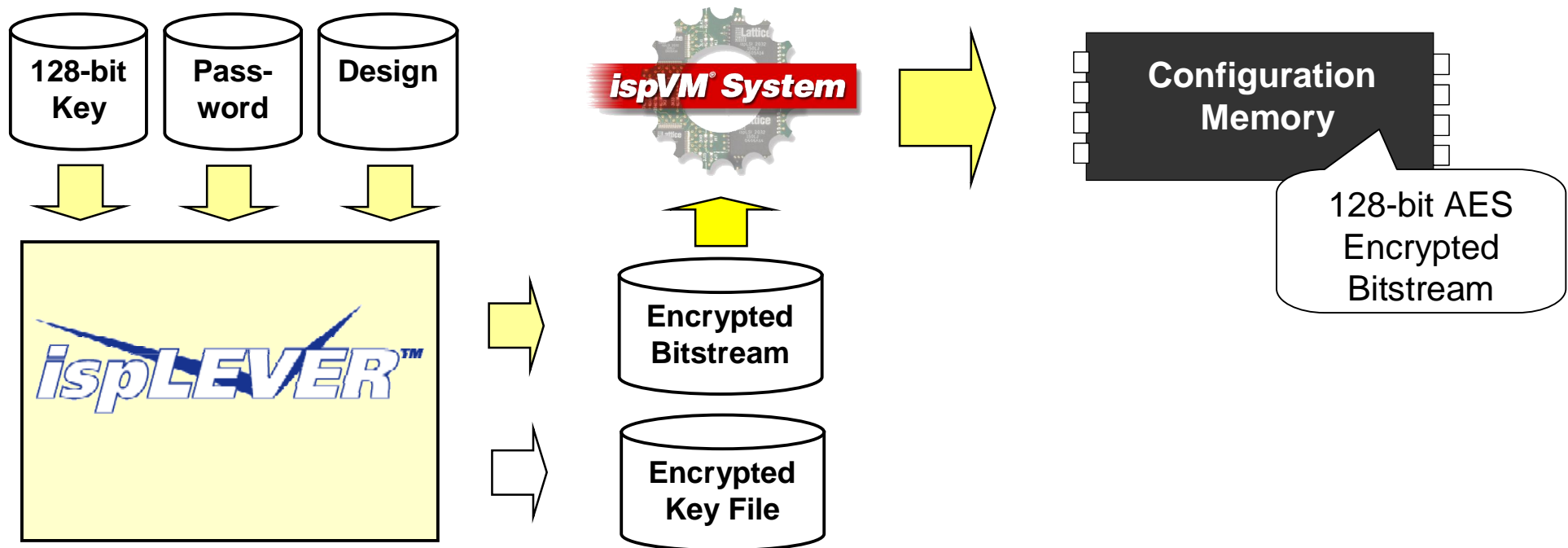
- ◆ Summary

Encryption Overview



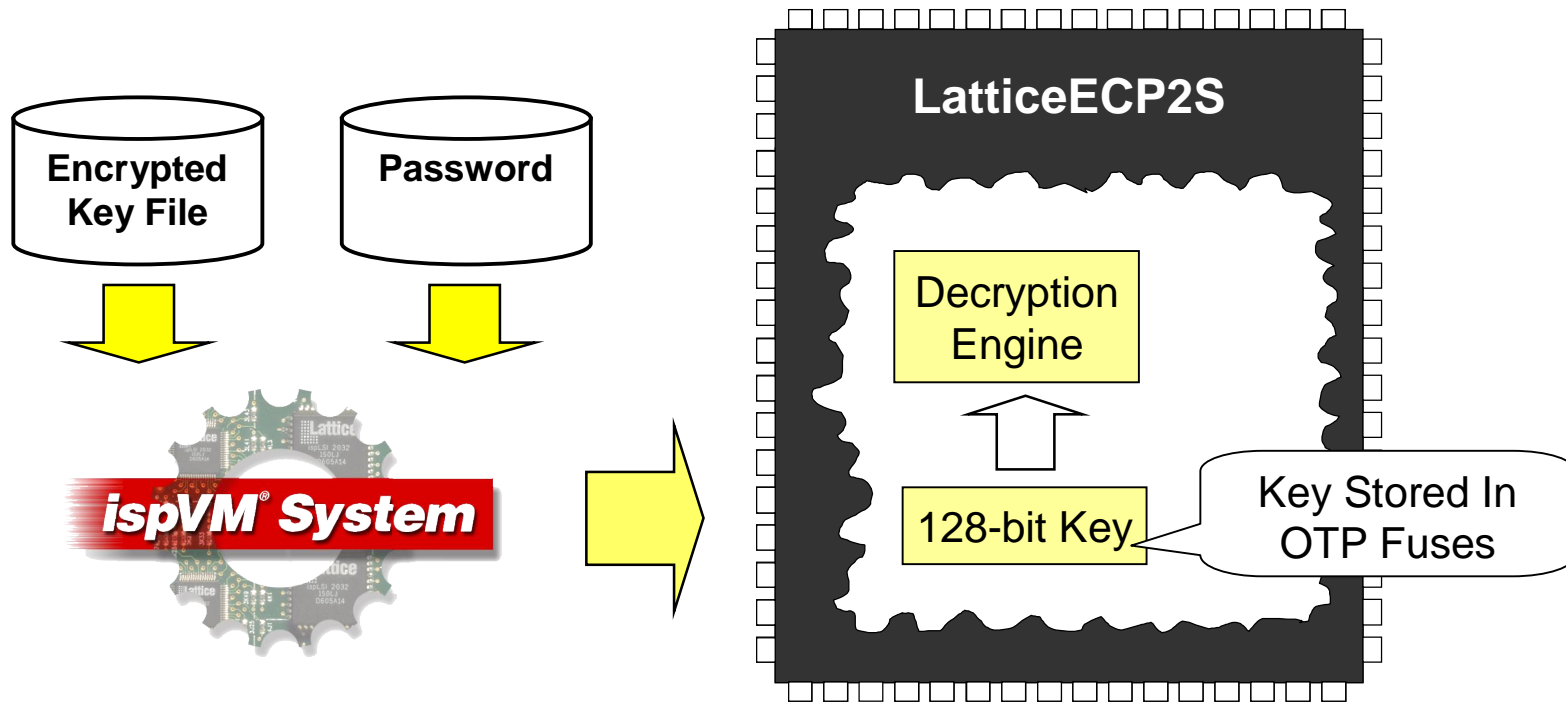
- ◆ **Design Security Increasingly Important**
 - Overbuilding, reverse engineering and cloning all too common
- ◆ **Optionally Encrypt Bitstreams With 128-bit AES Encryption Using ispLEVER**
- ◆ **On-Chip OTP (One Time Programmable) Fuses Store 128-bit Decryption Key**
 - More than one fuse per bit
 - Buried under 10 layers of metal
- ◆ **On-Chip 128-bit AES Decryption Engine**

Encryption – Step 1 (Bitstream Encryption)



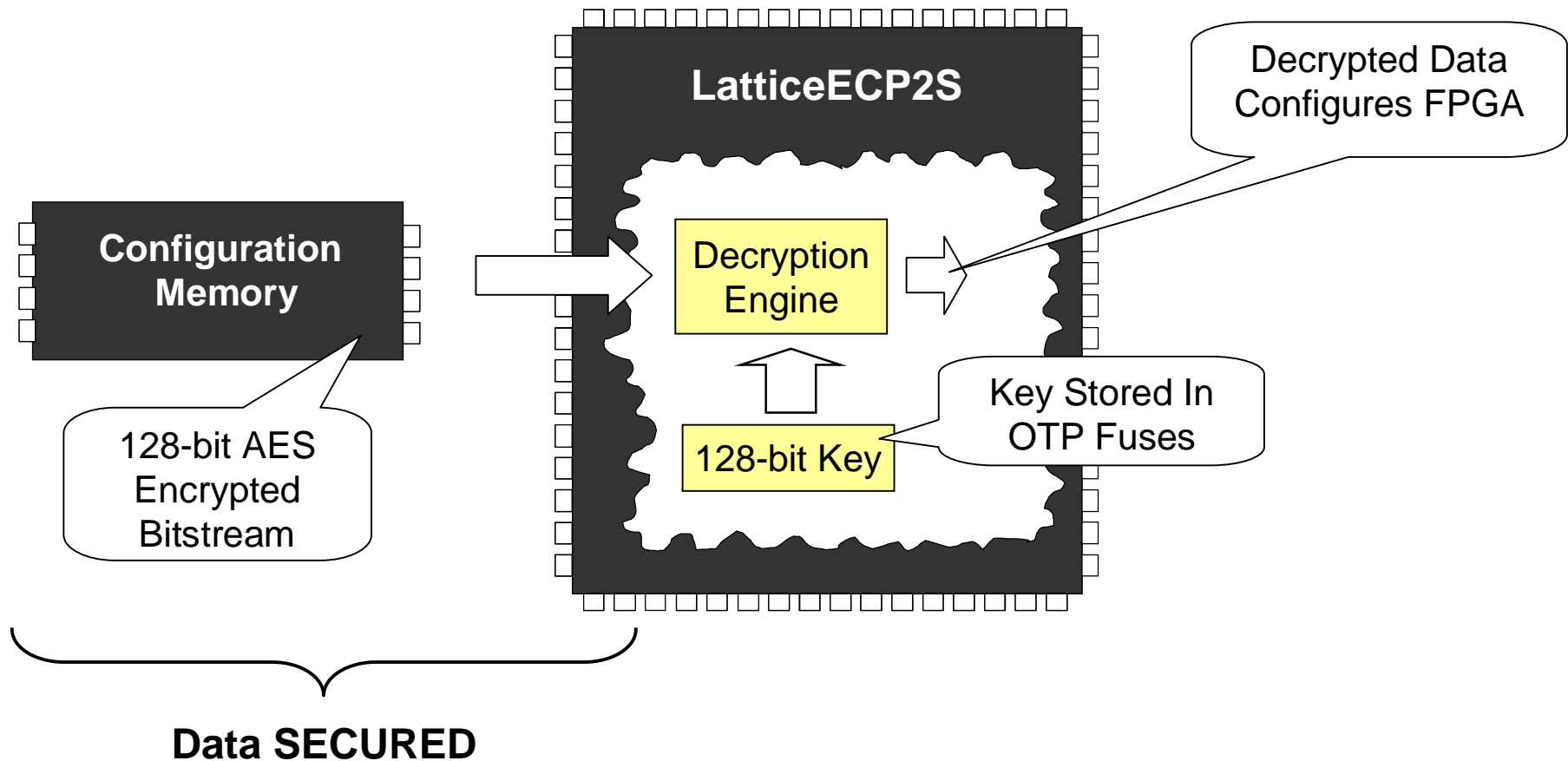
- ◆ **ispLEVER Encrypts Device Bitstream With 128-bit AES Encryption**
 - No encryption file size overhead for SPI bitstreams
 - Typically 25 to 50% file size overhead for non-SPI bitstreams
- ◆ **Encrypted Bitstream is Programmed Into Configuration Memory**
- ◆ **Encrypted Bitstream Only Works if LatticeECP2S Device is Programmed With Correct Decryption Key**

Encryption – Step 2 (Prog. On Chip Key Store)



- ◆ **ispVM Programs User Supplied 128-bit Key Into LatticeECP2S**
- ◆ **Key Stored In OTP Fuses**
 - Key protected from readback or physical examination
- ◆ **Once Encryption Key Is Programmed LatticeECP2S Will Only Operate With Correctly Encrypted Bitstream or an unencrypted Bitstream**

Encryption – Step 3 (Device Configuration)



- ◆ **At Power Up Encrypted Bitstream Is Loaded Into LatticeECP2S**
- ◆ **Bitstream Is Decrypted Using 128-bit AES Decryption Key**
 - **Stored In OTP Fuses**

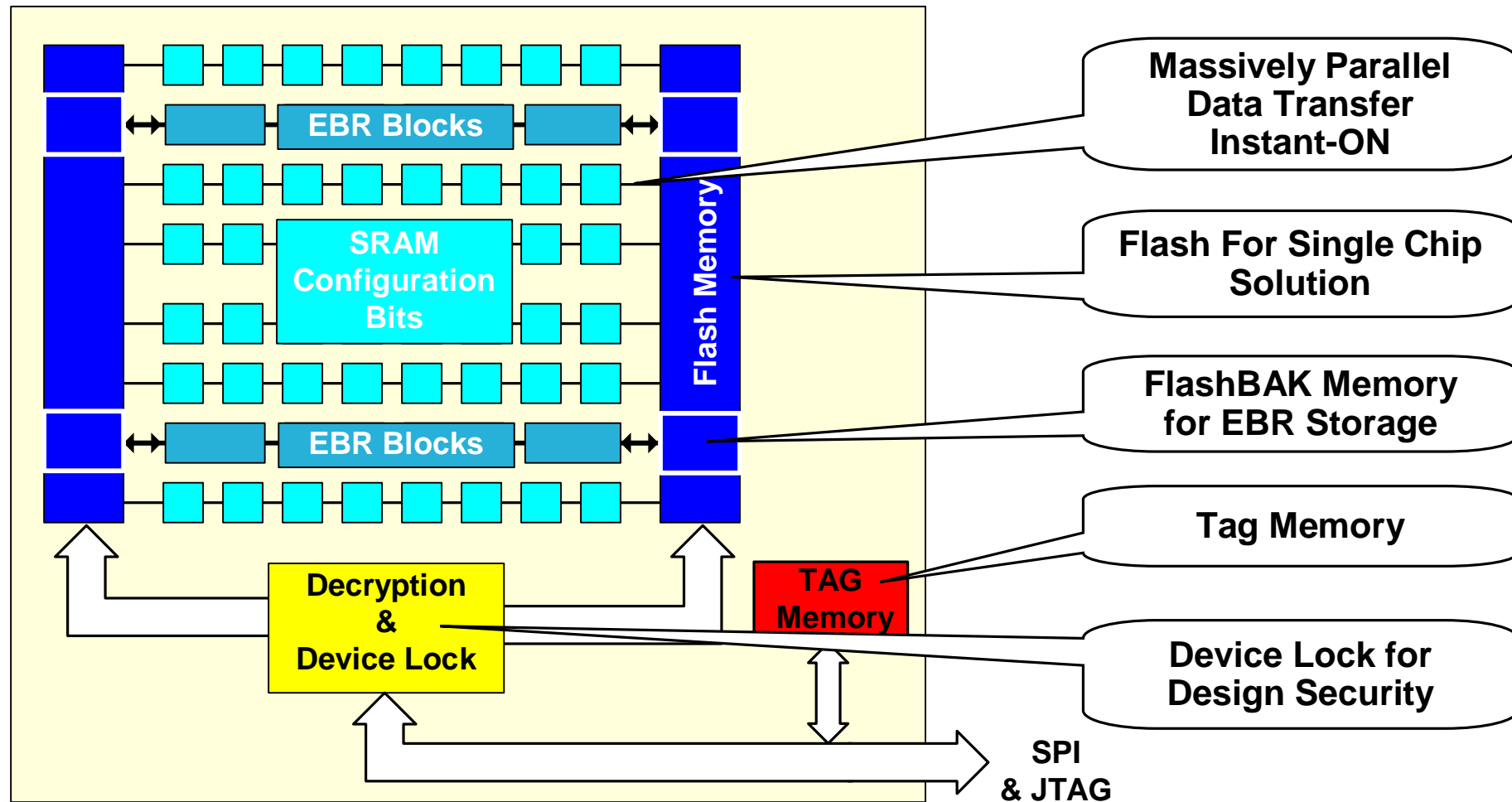
Lattice ECP2/M „S“ Device Family Overview

Device	ECP2						ECP2M				
	6	12	20	35	50	70	20	35	50	70	100
LUTs (K)	6	12	21	32	48	68	19	34	48	67	95
18x18 Multipliers	12	24	28	32	72	88	24	32	88	96	168
Distributed RAM (Kbits)	12	24	42	65	96	136	41	71	101	145	202
EBR SRAM Blocks	3	12	15	18	21	60	66	114	225	246	288
EBR Block SRAM (Kbits)	55	221	276	332	387	1106	1217	2101	4147	4534	5308
PLLs/DLLs	2/2	2/2	2/2	2/2	4/2	6/2	8/2	8/2	8/2	8/2	8/2
DDR1/DDR2 Memory (Mbps)	400/ 533	400/ 533	400/ 533	400/ 533	400/ 533	400/ 533	400/ 533	400/ 533	400/ 533	400/ 533	400/ 533
Package	I/O						SERDES/IO				
144-pin TQFP (20x20mm)	90	93									
208-pin PQFP (28x28mm)		131	131								
256-ball fpBGA (17x17mm)	190	193	193				4/140	4/140			
484-ball fpBGA (23x23mm)		297	331	331	339		4/304	4/303	4/270		
672-ball fpBGA (27x27mm)			402	450	500	500		4/410	8/372		
900-ball fpBGA (31x31mm)						583			8/410	16/416	16/416
1152-ball fpBGA (35x35mm)										16/436	16/520

Agenda

- ◆ Security Overview
- ◆ LatticeECP2S Device Security
- ◆ LatticeXP2 Device Security
- ◆ Summary

FlexiFlash Configuration Architecture



LatticeXP2 Security Overview

- ◆ **No External Bitstream**
- ◆ **Configuration Data Secured Within FLASH**
 - Buried under 10 layers of metal
 - Physical inspection does not reveal setting
- ◆ **Access Control Bits Provide Multiple Configuration Security Levels**
- ◆ **On-chip 128-bit Decryption Engine Allows Secure Reconfiguration of Flash**
- ◆ **TAG Memory Outside Security Schemes**

Access Control Settings

Config Secure Bit

On – Prevent readback

Off – Allow readback

Flash Protect

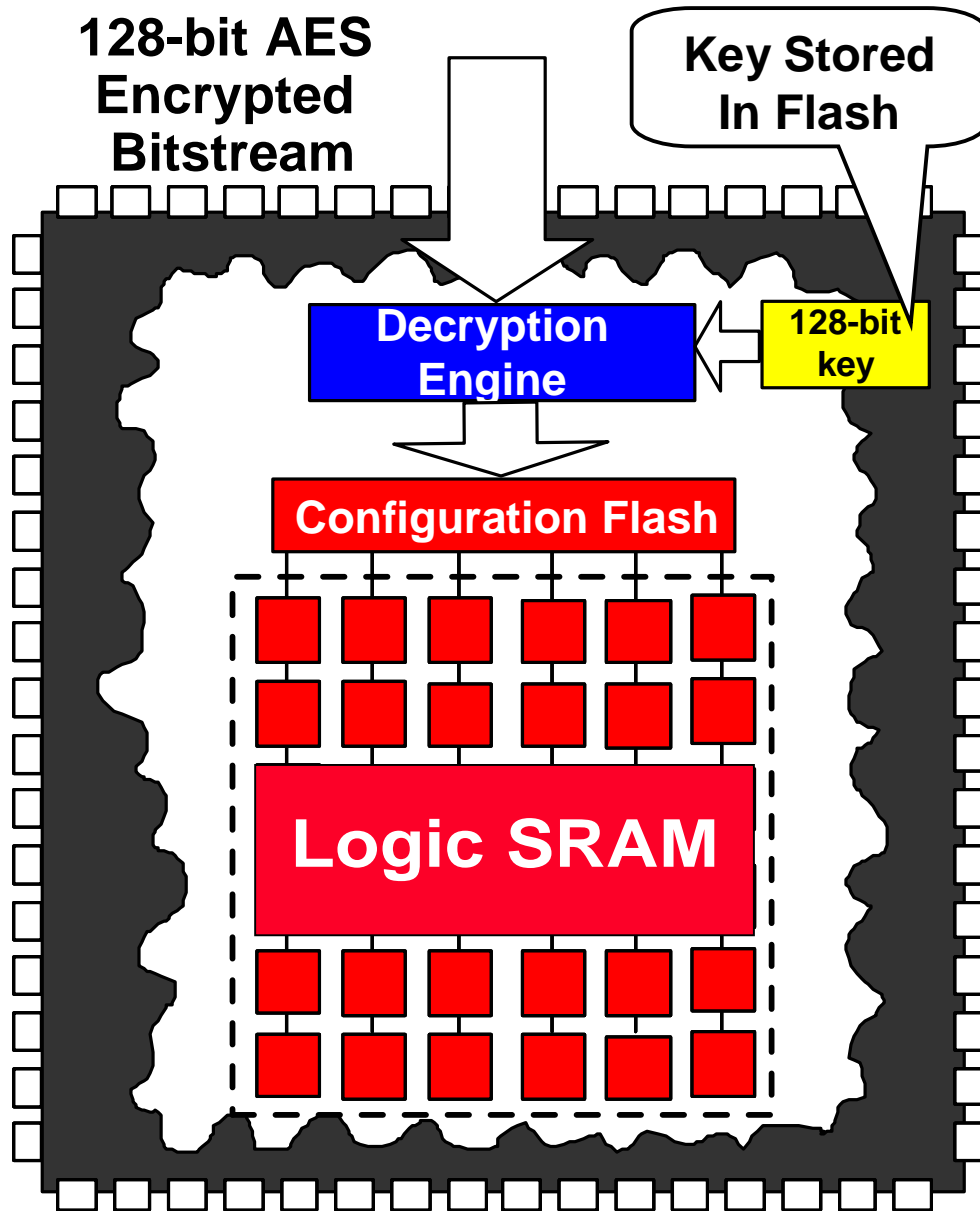
Off – Erase/write

Lock – Erase/write with key

OTP – No Erase/write

**Flexible Access Control Setting To Match
Your Use Conditions**

Programming Data Encryption



- ◆ **Design Security Important for Remote Updates:**
 - Avoid Theft of Your Intellectual Property
- ◆ **Optionally Encrypt Programming Data Using 128-bit AES Encryption**
- ◆ **On-chip Flash Stores 128-bit Decryption Key**
- ◆ **On-chip 128-bit AES Decryption Engine**

Lattice XP2 Device Family Overview

Device	XP2				
	5	8	17	30	40
LUTs (K)	5	8	17	29	40
18x18 Multipliers	12	16	20	28	32
Distributed RAM (Kbits)	10	18	35	56	83
EBR SRAM Blocks	9	12	15	21	48
EBR Block SRAM (Kbits)	166	221	276	387	885
PLLs/MDLLs	2/2	2/2	4/2	4/2	4/2
DDR1/DDR2 Memory (Mbps)	400	400	400	400	400
Package	I/O				
132-pin csBGA (8x8mm)	86	86			
144-pin TQFP (20x20mm)	100	100			
208-pin PQFP (28x28mm)	146	146	146		
256-ball fpBGA (17x17mm)	172	201	201	201	
484-ball fpBGA (23x23mm)			358	363	363
672-ball fpBGA (27x27mm)				472	540

Agenda

- ◆ Security Overview
- ◆ LatticeECP2S Device Security
- ◆ LatticeXP2 Device Security
- ◆ Summary

Lattice Devices Protect Your Designs

◆ Security Increasingly Important

- Theft of service, reverse engineering, cloning and overbuilding common concerns

◆ Lattice ECP2/M Provide Low Cost FPGAs With 128-bit AES Bitstream Encryption up to 95K LUTs

- Strong defense against piracy

◆ LatticeXP2 Provide Ultimate Non-volatile FPGA Solutions up to 40K LUTs

- No external bitstream at power-up
- Readback protection
- Flash configuration protection
- Secure channel for device updates

Esencrypt AES Core implementation in ECP2/M

LFE2-50SE-5F672C

Speed Grade: -5

Package: FPBGA672

Typ	Slices	F_max	encrypt		decrypt	
			clk/Op	MB/s	clk/Op	MB/s
AES Small	1058 (4%)	41 MHz	53	12,4	95	6,9
AES Quick	2183 (9%)	34 MHz	12	45,3	24	22,7
AES Pipeline*	14021 (42%)	42,8MHz	1	684,8	1	684,8

*AES Pipeline for -7 Speed Grade (53.3MHz=>852 MB/s), with modifications >1000MB/s possible