Crypto Hardware Accelerator Design and Rapid Chips Design & Fabrication Platform

Makoto Ikeda
Systems Design Lab,
The University of Tokyo, Tokyo, Japan

Acknowledgment

This work was supported by the Cabinet Office (CAO), Cross-ministerial Strategic Innovation Promotion Program (SIP), “Cyber Physical Security for IoT Society”, JPNP18015 (funding agency: NEDO), the New Energy and Industrial Technology Development Organization (NEDO), and Council for Science, Technology and Innovation (CSTI), Crossrministerial Strategic Innovation Promotion Program (SIP), “Cyber-Security for Critical Infrastructure” (funded by NEDO). Agile-X Project is supported by MEXT.
The VLSI chip is designed and fabricated through VDEC, the University of Tokyo in collaboration with Cadence, Synopsys, Mentor Graphics (Siemens EDA), and Renesas Electronics Corp.

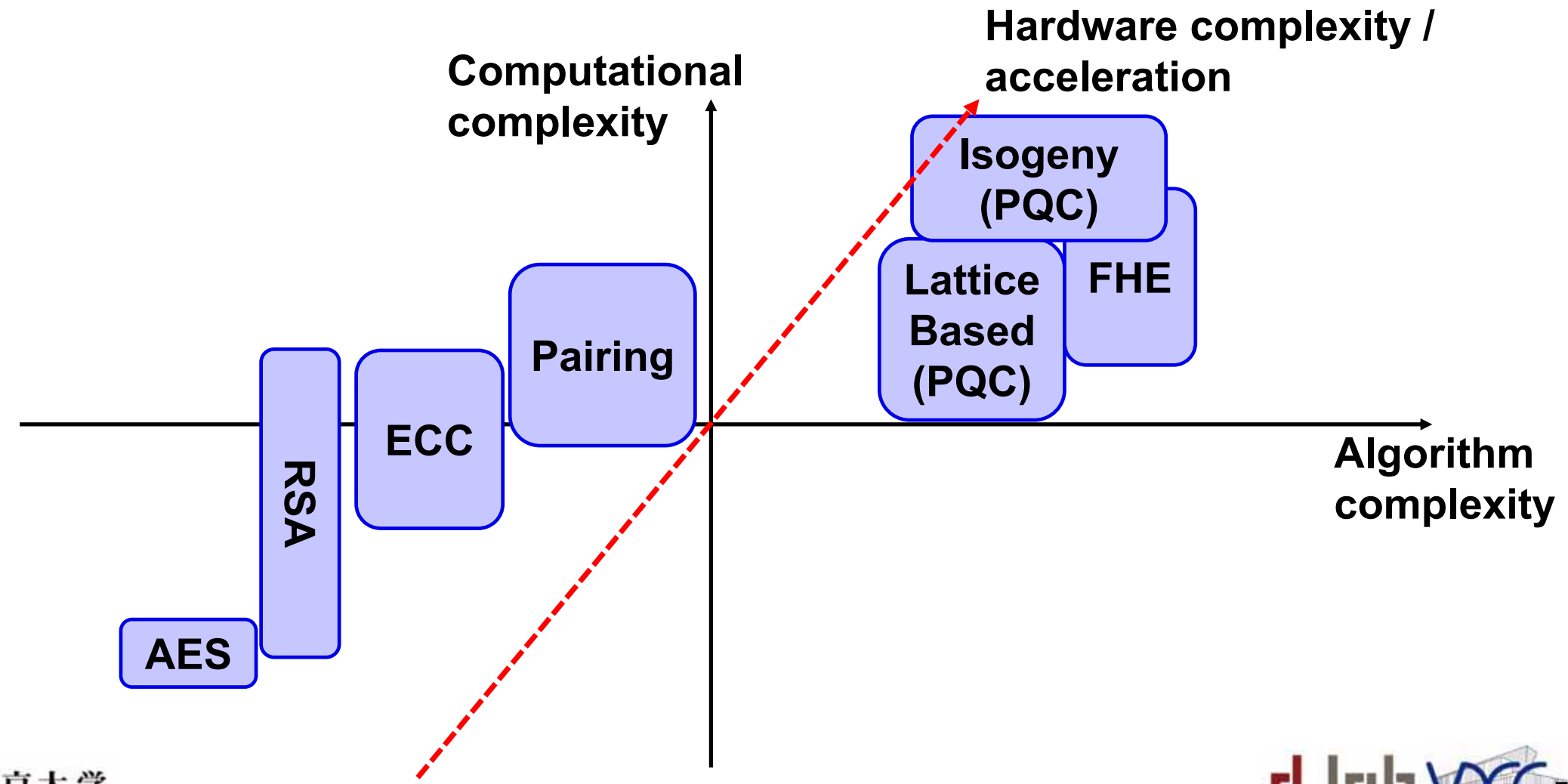
Agenda

- **Background**
  - ✓ **Overview of Hardware Acceleration of Crypto-Algorithms, and Functionality**
- **Design Space Exploration of Crypto-Algorithm to Hardware**
  - ✓ **ECC Accelerator Design and Design space Exploration**
  - ✓ **Template-based Design Automation**
- **Introduction to d.lab, chip design platform for Japanese Academia**
  - **Agile-X Project ~Democratizing Chip Design~**
- **Conclusions**

Why hardware acceleration?

- **Completely digital…Possibility for performance scaling by advance process**
  - **Advanced complex algorithms, which is now regarded as useless because of slow performance, come true (e.g.: LDPC)**
- **Optimized hardware can easily applicable to tiny IoT edge devices, so that public-key/functionality can be everywhere**

Encryption/Digital Signature Algorithms

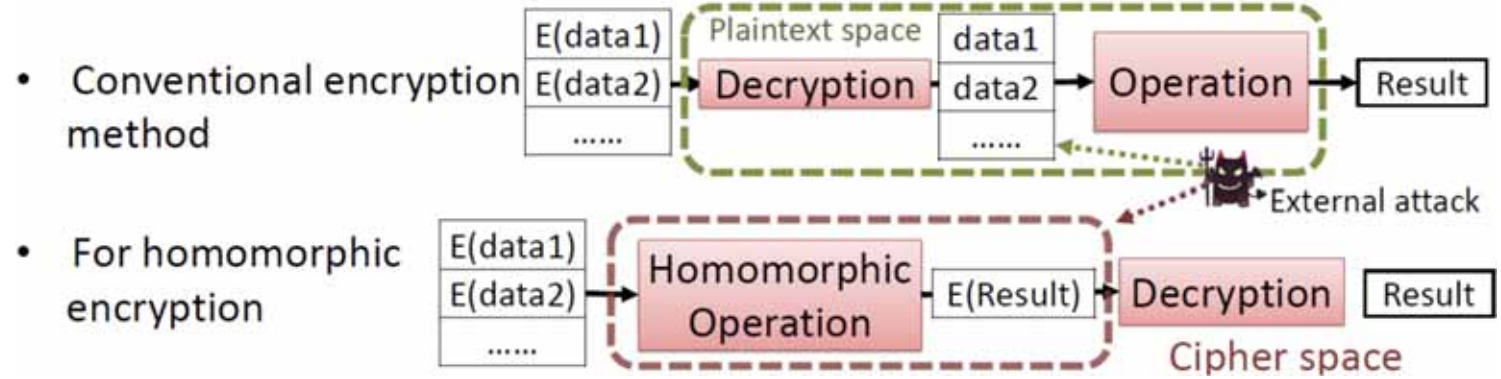


Advanced Encryption (Functional Encryption)

Encryption method	Functionality
Attribute/ID base encryption / functional encryption	Access control by attributes on plain text and on decryptor
Searchable encryption	Searchable in cypher space
Proxy re-encryption	Re-encryption for other decryptor without through plain text
Broadcasting encryption	Encryption with access control for multiple decryptors
Threshold encryption	Decryptable with data above threshold
Time release encryption	Encryption with access control by time

Signature method	Functionality
Attribute/ID base signature	Digital signature with access control of authentication by attributes
Threshold signature	Decryptable with signatures above threshold
Group signature	Digital signature with encryptor anonymization
Blind signature	Digital signature with message concealment
Multiple signature / aggregate signature	Signature compression, and bundle signature authentication
Time release signature	Digital signature with access control by time

Homomorphic Encryption

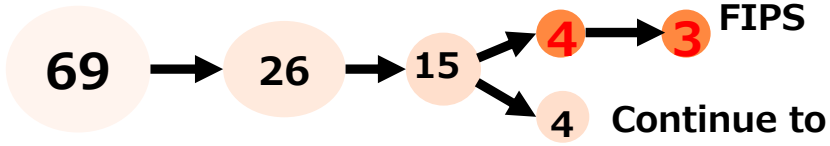


Type	Supported Operations	Representative Encryption method
Additive Homomorphism	+	Paillier Encryption
Multiplicative Homomorphism	X	RSA Encryption
Fully Homomorphism	+, X	Ring-LWE based

Additive Homomorphism

Post Quantum Encryption (NIST)

Number of candidate algorithms for Post-quantum Cryptography (PQC)



3rd Round Finalists

Key Exchange Mechanism (KEM) & Encryption

Name	Type
Classic McEliece	Code-base
Crystals-Kyber	**Lattice-base** **FIPS-203 MLB-KEM**
NTRU	Lattice-base
SABER	Lattice-base

Alternate Candidates

Key Exchange Mechanism (KEM) & Encryption

Name	Type
BIKE	Code-base
FrodoKEM	Lattice-base
HQC	Code-base
NTRU Prime	Lattice-base
SIKE	Isogeny-base

Digital Signature Authentication

Name	Type
Crystals-Dilithium	**Lattice-base** **FIPS-204 MLB-DSA**
FALCON	**Lattice-base**
Rainbow	Polynomial-base

Digital Signature Authentication

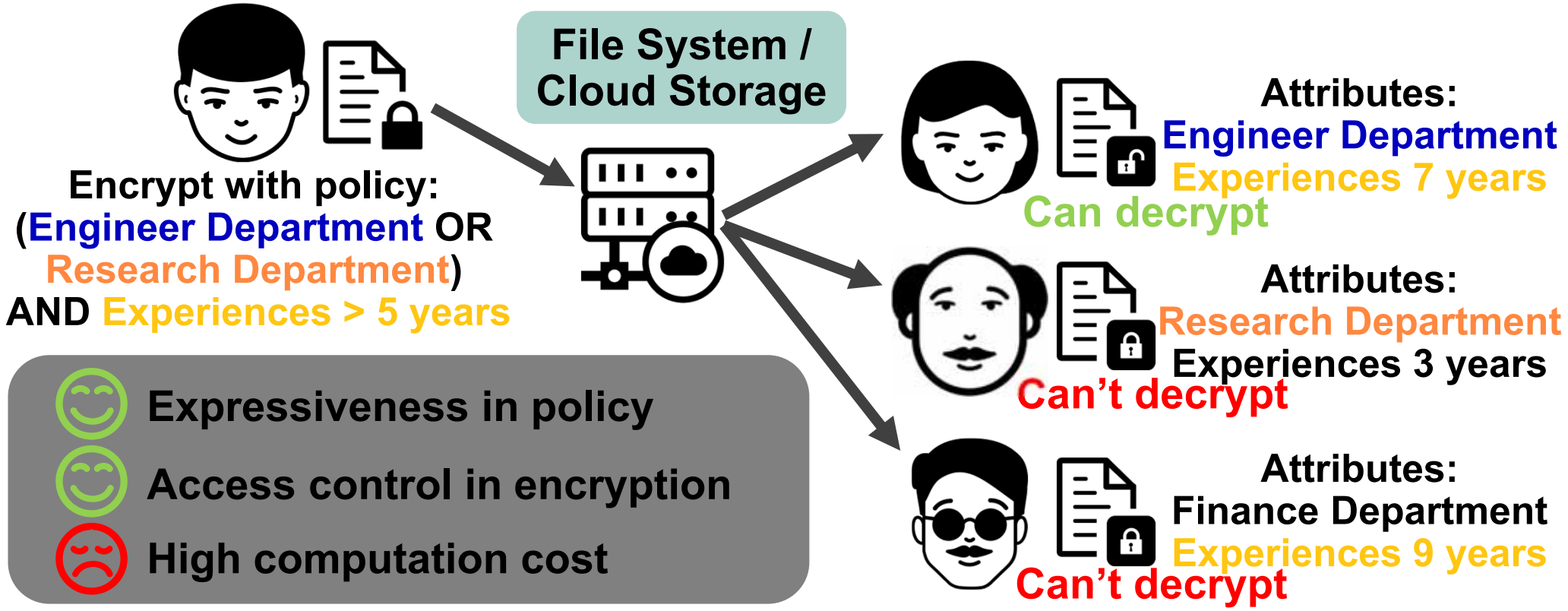
Name	Type
GeMSS	Polynomial-base
Picnic	Shard-key-base
SPHINCS+	**Hash-base** **FIPS-205 SHB-DSA**

2nd Round for DSA Standards

Name	Type
CROSS	Code-base
FAEST	Symmetric-base
HAWK	Lattice-base
LESS	Code-base
MAYO	Multivariate
Mirath	MPC-in-the-Head
MQOM	MPC-in-the-Head
PERK	MPC-in-the-Head
QR-UOV	Multivariate
RYDE	MPC-in-the-Head
SDitH	MPC-in-the-Head
SNOVA	Multivariate
SQIsign	Isogeny-base
UOV	Multivariate

Attribute-based Encryption

Ciphertext-based ABE (CP-ABE) Example in File Sharing Scenario



Elliptic Curve-based Functions

G1_MUL	Elliptic Curve Scalar Multiplication computed with Montgomery Ladder
G1_HASH	Map string to a point on the curve
G2_MUL	Similar to G1_MUL but executed on G2
GT_EXP	Similar to G1_MUL, but is an exponentiation on GT
Pairing	A bilinear map mapping a point on G1 and a point on G2 to GT

Elliptic Curve

- Curve of the form $y^2=x^3+ax+b$ where $4a^3+27b^2\neq 0$
  - Pairing friendly: BLS12-381 curve

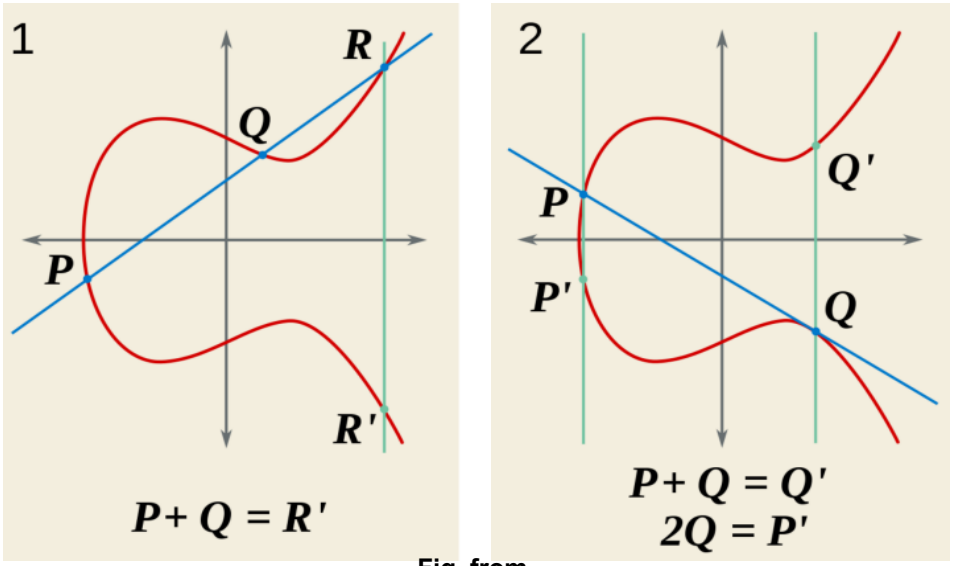


Fig. from
https://commons.wikimedia.org/w/index.php?curid=2970564

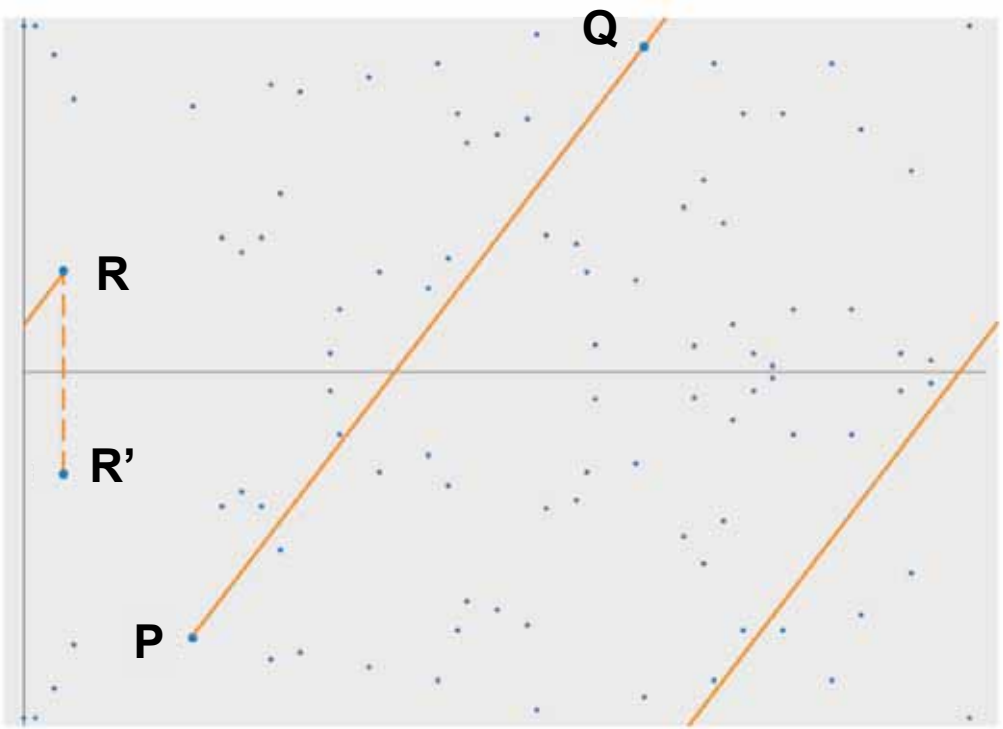


Fig. from https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

- Elliptic Curve Scalar Multiplication
  - Q = [k]P = P + P + … + P (k times)

Elliptic Curve Discrete Logarithm Problem

Higher Extension Fields

- **Similar to imaginary number concept**

BLS12-381 Curve on $\mathbb{F}_p$:

$E(\mathbb{F}_p) : y^2=x^3+4$

BLS12-381 Curve on $\mathbb{F}_{p^2}$:

$E'(\mathbb{F}_{p^2}) : y^2=x^3+4(1+i)$

G1 $\subset E(\mathbb{F}_p)$

G2 $\subset E'(\mathbb{F}_{p^2})$

Extension 2

GT $\subset \mu_r \in \mathbb{F}_{p^{12}}$

Extension 12

Computation Loads

Agenda

- Background
  - ✓ Overview of Hardware Acceleration of Crypto-Algorithms, and Functionality
- Design Space Exploration of Crypto-Algorithm to Hardware
  - ✓ ECC Accelerator Design and Design space Exploration
  - ✓ Template-based Design Automation
- Introduction to d.lab, chip design platform for Japanese Academia
  - Agile-X Project ~Democratizing Chip Design~
- Conclusions

Cryptography based on Elliptic Curve

Define point addition and point doubling over Elliptic curve

↓

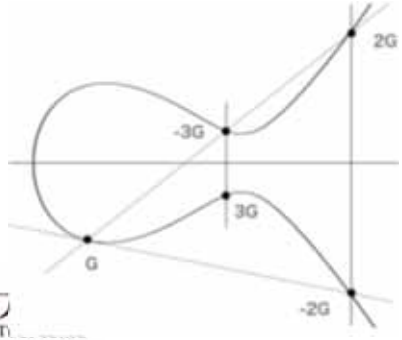
Realize multiple of k(scaler) of base point G, by combination of add and doubling

↓

kG → k: discrete logarithm problem on elliptic curve (ECDLP)

↓

Secure signature generation based on ECDLP

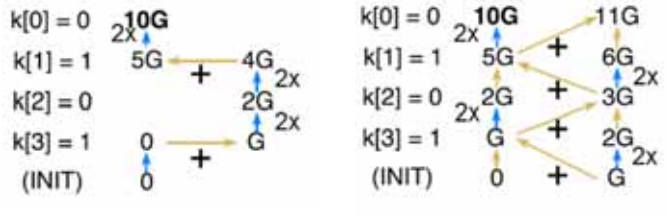


Basic operation: "Scaler Multiplication" to obtain kG from scaler k and base point G

$$Q = kG = \sum_{i=0}^{n-1} k_{i-1} \cdot 2^{i-1} G$$

Point multiplication:

LtR(RtL) / Montgomery Ladder



Point doubling:
k=2: 2G = 2*G

$$G_1(x_1, y_1) + G_2(x_2, y_2) \rightarrow G_3(x_3, y_3)$$

$$x_3 = \lambda_3^2 - x_2 - x_1$$

$$y_3 = \lambda_3(x_1 - x_3) - y_1$$

$$\lambda_3 = \frac{y_2 - y_1}{x_2 - x_1}$$

Point addition:
k=3: 3G = G + 2G

$$2G_1(x_1, y_1) \rightarrow G_4(x_4, y_4)$$

$$x_4 = \lambda_4^2 - 2x_1$$

$$y_4 = \lambda_4(x_1 - x_4) - y_1$$

$$\lambda_4 = \frac{3x_1^2 + a}{2y}$$

Assuming Short Weierstrass Curves:

$$Y^2 = x^3 + ax + b$$

- **Affine Coordinate**
  - ✓ **Requires division**

$$(x_i, y_i)$$

- **Projective Coordinate:**
  - ✓ **Good for point addition**

$$(x_i, y_i) = \left(\frac{X_i}{Z_i}, \frac{Y_i}{Z_i}\right)$$

- **Jacobian Coordinate:**
  - ✓ **Good for point doubling**

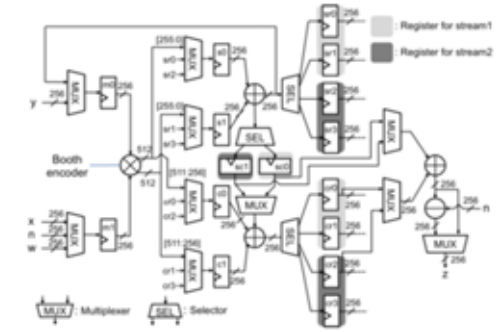
$$(x_i, y_i) = \left(\frac{X_i}{Z_i^2}, \frac{Y_i}{Z_i^3}\right)$$

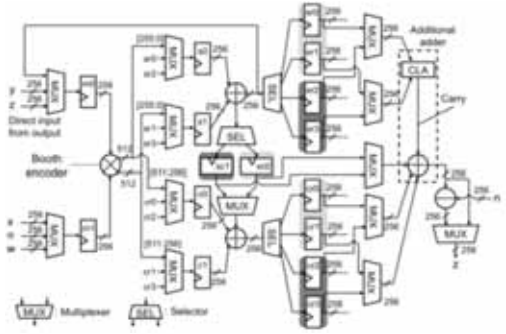
- **XZ Coordinate:**
  - ✓ **Smallest if no need for Y**

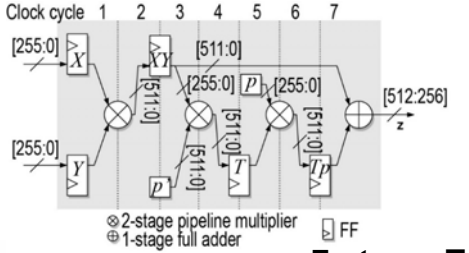
$$(x_i) = \left(\frac{X_i}{Z_i}\right)$$

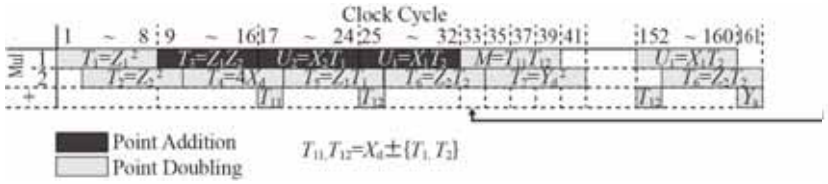
Selection of radix of data-path:
1bit (bit serial),,, up to full bit (256 bit)

Architecture Exploration & Scheduling



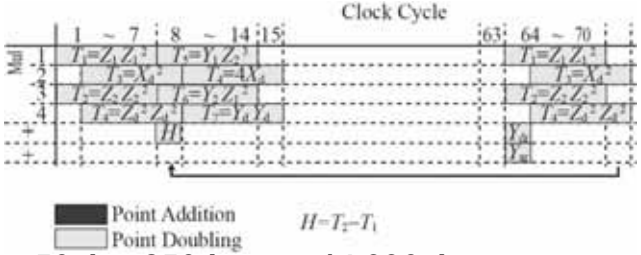






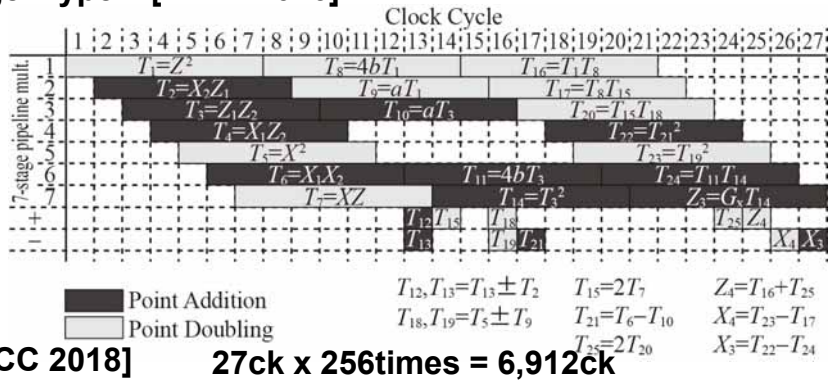
128ck x 256times = 32,768ck

8-stage: Type 1 [A-SSCC 2016]



56ck x 256times = 14,336ck

7-stage: Type 2 [IEICE 2016]



7-stage: Type 3 [A-SSCC 2018]

27ck x 256times = 6,912ck

Require:
$X, Y \in \mathbb{F}_p$,
$R = 2^{\lfloor \log_2 p \rfloor}$,
$p' = -p^{-1} \bmod R$
Ensure: $Z = XYR^{-1} \bmod p$
1: $T \Leftarrow (XY \bmod R) \cdot p' \bmod R$
2: $Z \Leftarrow (XY + Tp)/R$
3: **if** $Z \geq p$ **then**
4: $\quad Z \Leftarrow Z - p$
5: **end if**
6: **return** Z

Equation and Scheduling

Case 1

Assumptions: 4*a24=a+2

Cost: 6M + 4S + 1*a24 + 8add

$A = X2+Z2$
$AA = A^2$
$B = X2-Z2$
$BB = B^2$
$E = AA-BB$
$C = X3+Z3$
$D = X3-Z3$
$DA = D*A$
$CB = C*B$
$X5 = Z1*(DA + CB)^2$
$Z5 = X1*(DA - CB)^2$
$X4 = AA*BB$
$Z4 = E*(BB+a24*E)$

Curve 25519

Case 2

Assumptions: 4*a24=a+2

Cost: 8M + 4S + 1*a24 + 7add

$t0 = X3 - Z3$
$t1 = X2 + Z2$
$t2 = X3 + Z3$
$t3 = X2 - Z2$
$t4 = t2 * t3$
$t5 = t0 * t1$
$t6 = t5 + t4$
$t7 = t6 \hat{} 2$
$X5 = Z1 * t7$
$t8 = t5 - t4$
$t9 = t8 \hat{} 2$
$Z5 = X1 * t9$
$t10 = t1 \hat{} 2$
$t11 = t3 \hat{} 2$
$X4 = t10 * t11$
$t12 = X2 * Z2$
$t13 = 4 * t12$
$t14 = a24 * t13$
$t15 = t11 + t14$
$Z4 = t13 * t15$

Case 3

Cost: 10M + 5S + 1*a24 + 5add

$t0 = Z2 * Z3$
$t1 = X2 * X3$
$t2 = t1 - t0$
$t3 = t2 \hat{} 2$
$X5 = Z1 * t3$
$t4 = Z2 * X3$
$t5 = X2 * Z3$
$t6 = t5 - t4$
$t7 = t6 \hat{} 2$
$Z5 = X1 * t7$
$t8 = X2 \hat{} 2$
$t9 = Z2 \hat{} 2$
$t10 = t8 - t9$
$X4 = t10 \hat{} 2$
$t11 = X2 * Z2$
$t12 = a * t11$
$t13 = t8 + t12$
$t14 = t13 + t9$
$t15 = Z2 * t14$
$t16 = X2 * t15$
$Z4 = 4 * t16$

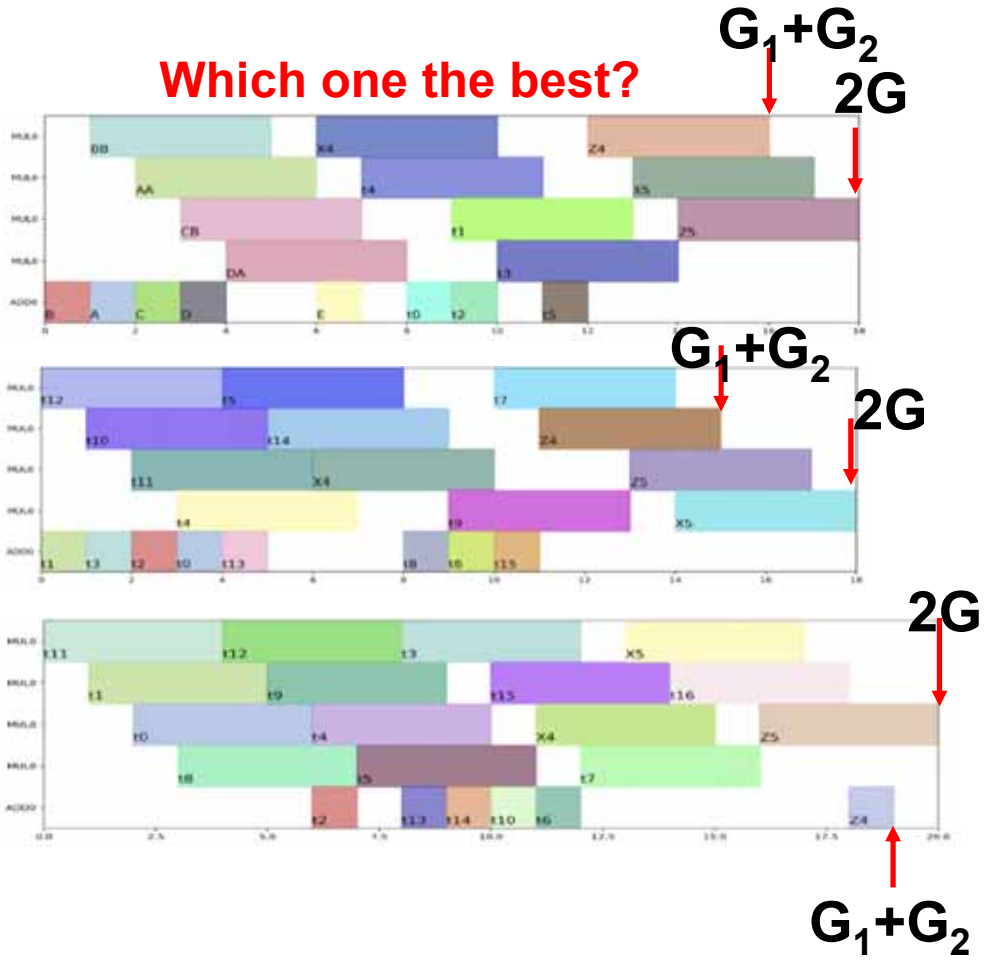
Which one the best?

Which one the best?

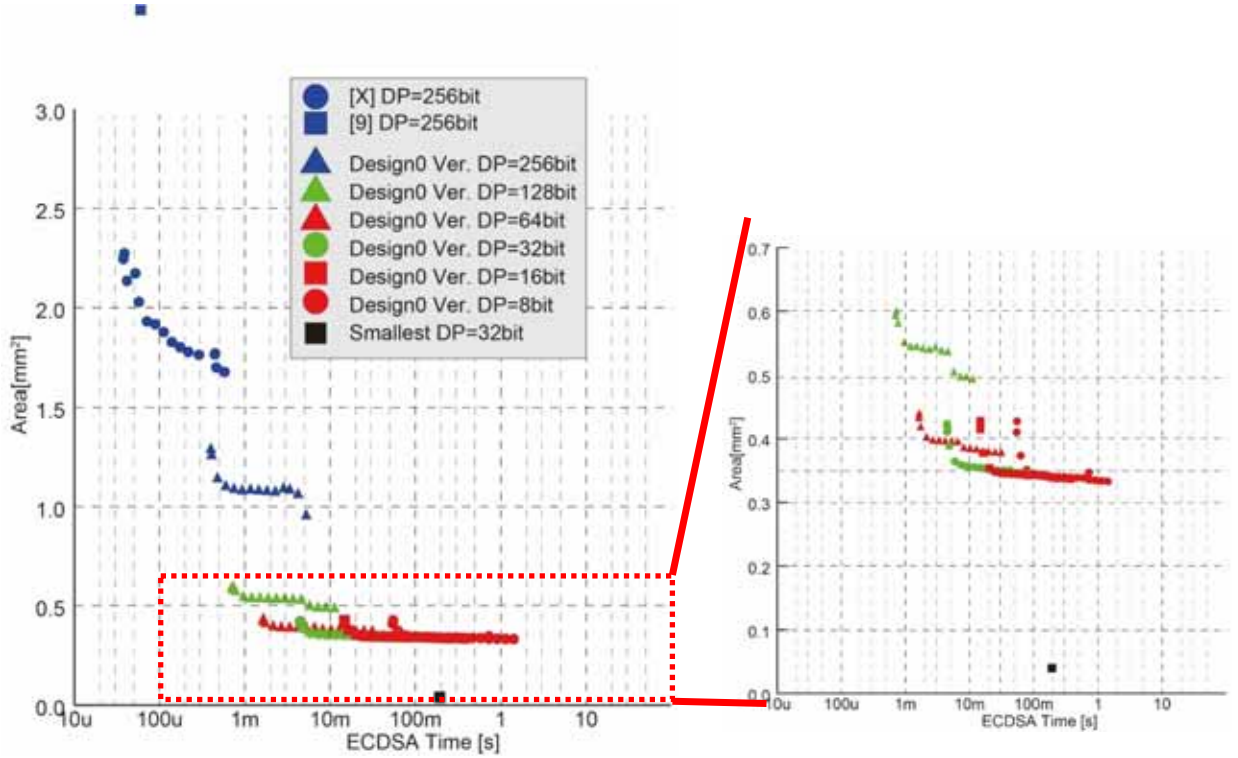
Case 1

Case 2

Case 3

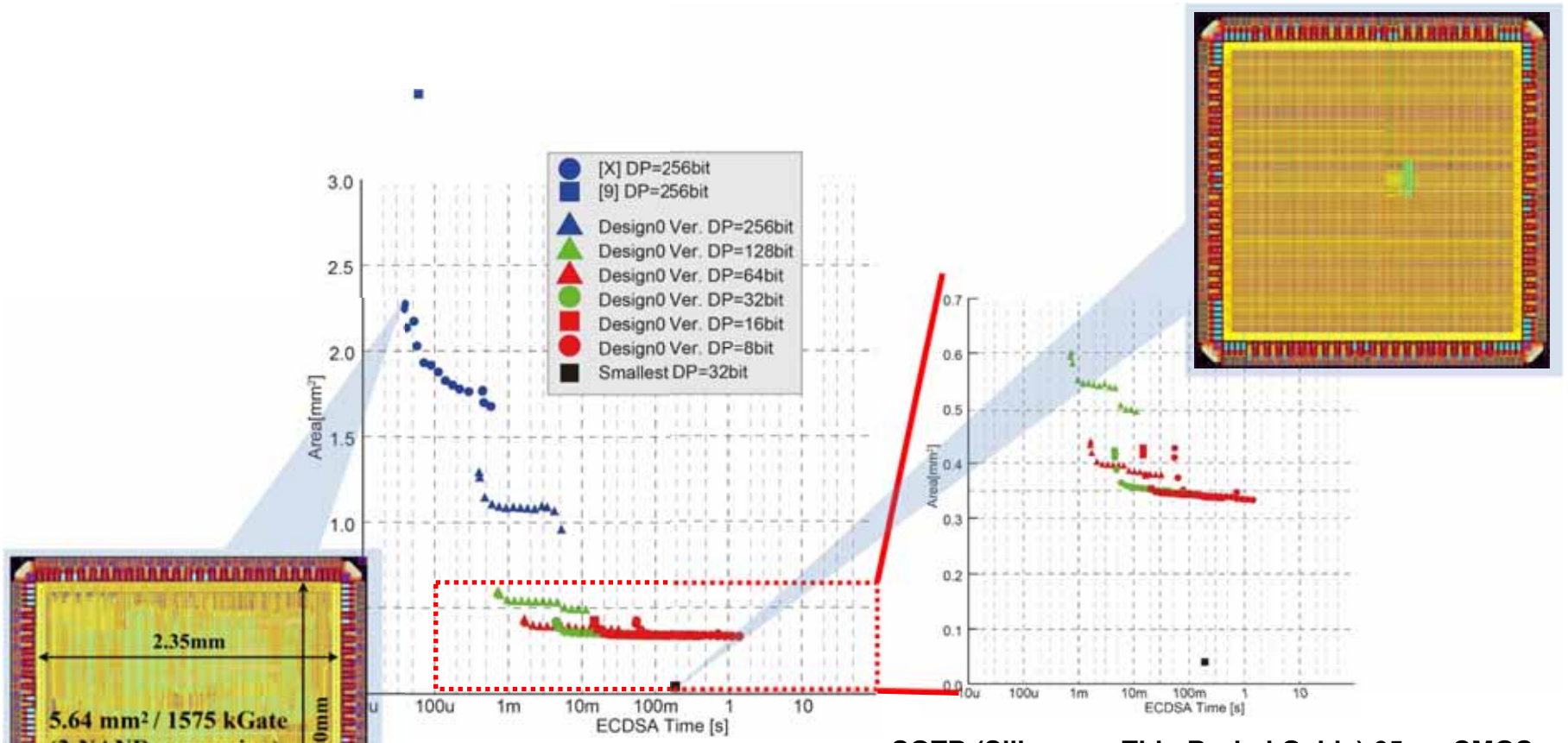


Design Space Exploration: Word Size



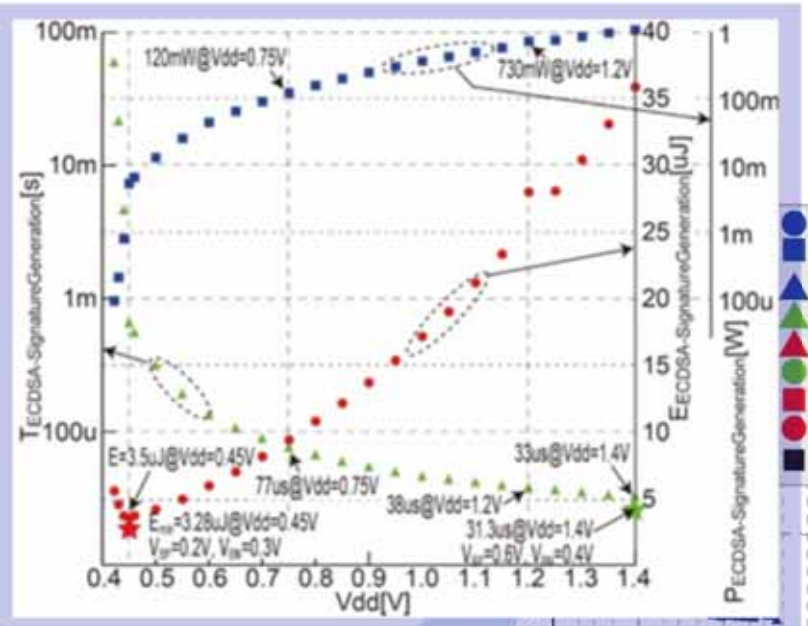
SOTB (Silicon on Thin Buried Oxide) 65nm CMOS

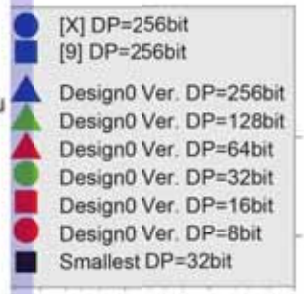
Design Space Exploration: Example designs

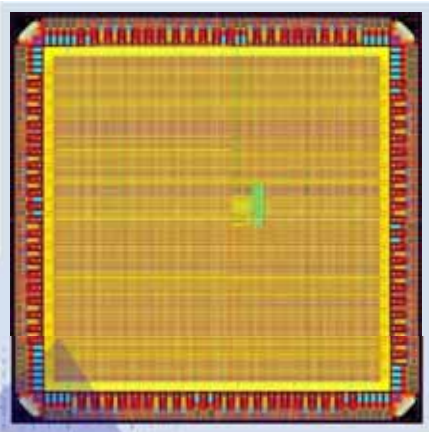


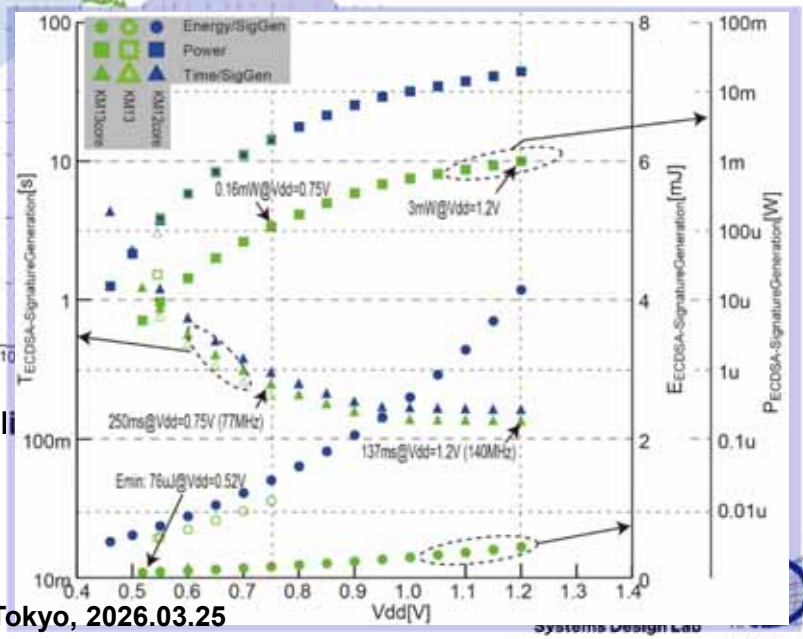
SOTB (Silicon on Thin Buried Oxide) 65nm CMOS

Design Space Exploration: Measured results







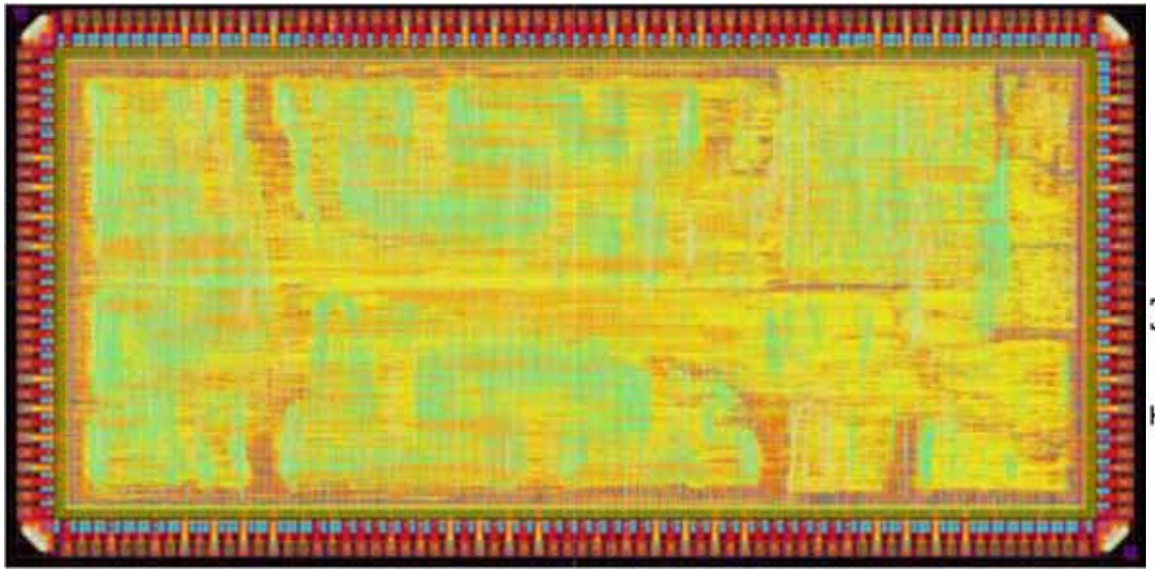


Comparisons

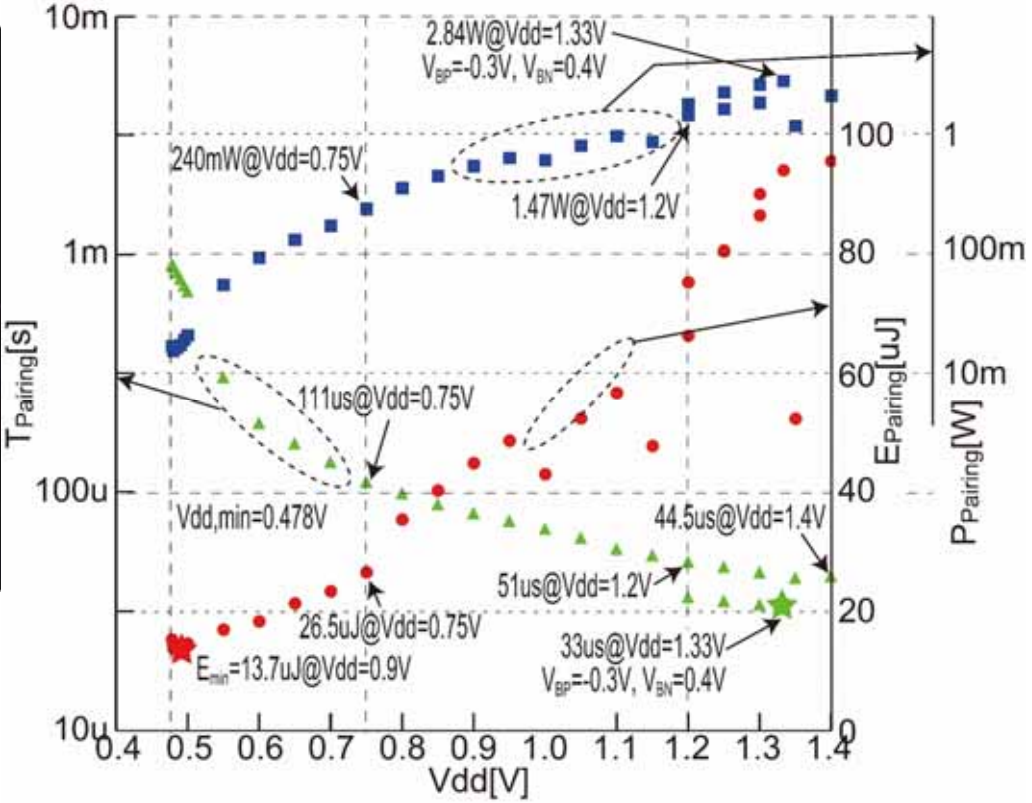
	Plat.	#Gate [kG]	Area [mm^2]	#Clk	Vdd [V]	Freq [MHz]	Tsg [ms]	Pow. [mW]	E [uJ]	Enc/kG	Enc/ uJ
Ours 2018	65nm	13	0.03	19.4M	0.75	77	250	**0.16**	100	0.31	0.04
Ours 2018 [1]	65nm	1,580	5.64	**7.5k**	0.45	35.7	0.21	15.6	**3.28**	3.01	**1,452**
					0.75	98.0	0.076	123	9.32	8.33	**1,412**
					1.4	238	**0.031**	1,227	38.7	**20.4**	834
Ours 2016 [2]	65nm	2,500	--	15k	--	236	0.06	--	--	6.67	--
Ours 2016 [3]	65nm	1,370	1.92	34.7k	0.25		11	0.15	1.68	0.07	54.1
					0.3		2.3	0.69	1.68	0.32	259
					1.1		0.33	42.9	13.9	2.21	218
2012 [4]	90nm	540	2.72	22.3k	--	131	0.17	--	--	10.9	--
2010 [5]	Stratix II (90nm)	9,177ALM+96DSP	--	107k	--	157	0.32	--	--	--	--
2018 [6]	AMD EPYC7601 (14nm)	NA (64-thread)	NA	157.4k		2.2-3.2GHz	0.072	180,000	12,900	--	--

[1] S Sugiyama, A-SSCC 2018, [2] M. Tamura, IEICE T. Fund. v. 99EA, No. 12, pp. 2444-2452, 2016, [3] M. Tamura, A-SSCC 2016, pp. 341-344, 2016,
[4] S.C. Chung, ISCAS2012, pp. 1456-1459, 2012, [5] N. Guillermin, CHES 2010, pp. 48-64, 2010, [6] bench.cr.yp.to/results-sign.html, Oct. 2018

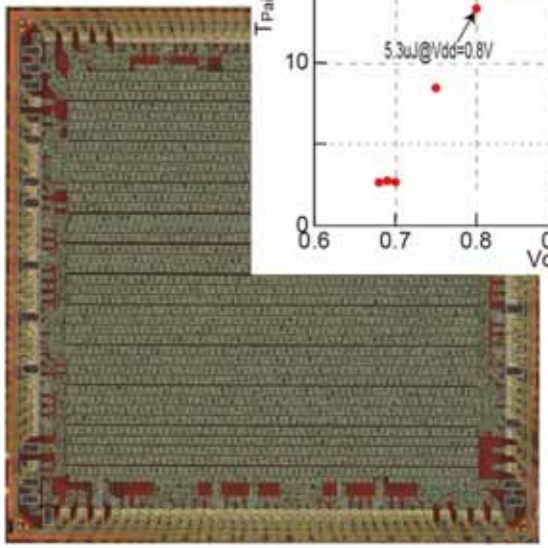
Chip Implementation in 65nm CMOS

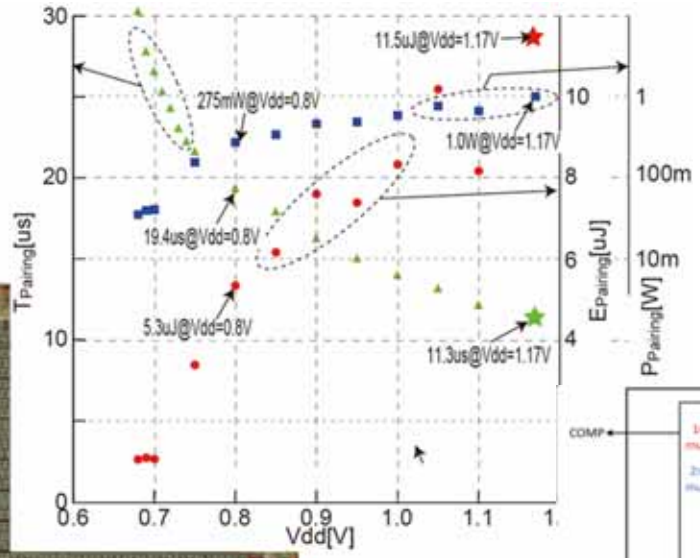


- SOTB 65nm CMOS process
- Effective gate count : 2,790k (2-NAND)
- Chip area : 12.8 mm^2



Performance Acceleration





- TSMC 12nm FINFET
- Effective gate count : ~2,790k
- Chip area : 2.6 mm^2

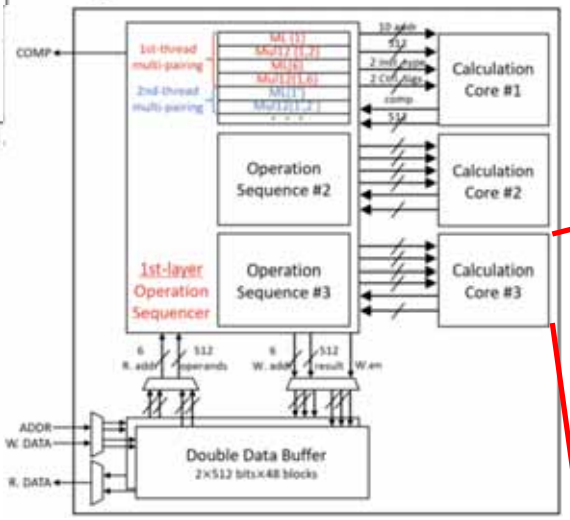
For the case of multi-pairing: Multi-core

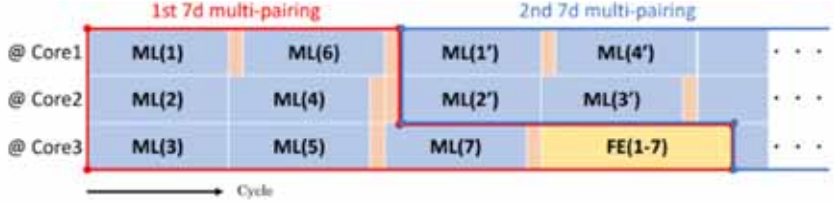
$$f_i = \mathrm{ML}(Q_i, P_i)$$

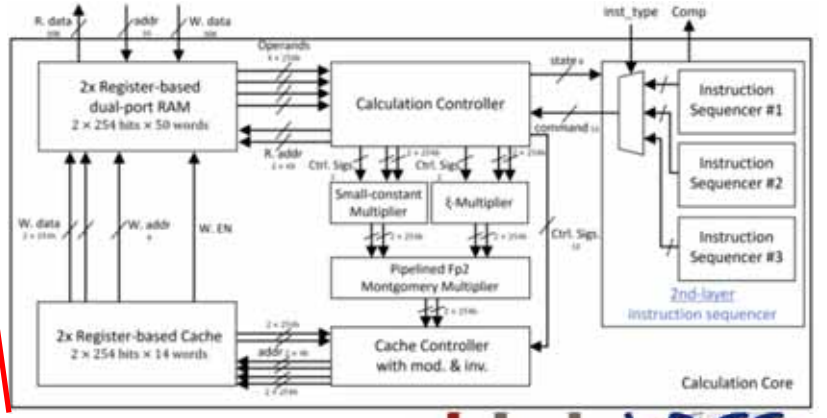
$$a_i = \mathrm{FE}(f_i) = f_i^{(p^6-1)(p^2+1)(p^4-p^2+1)/r}$$

$$a = \prod_{i=0}^{n} a_i = a_{\mathrm{opt}}(Q_1,\ P_1)\cdots a_{\mathrm{opt}}(Q_n,\ P_n).$$

$$a = \mathrm{FE}\left(\prod_{i=0}^{n} \mathrm{ML}(Q_i,\ P_i)\right)$$







Comparisons

BN12

Platform	#Gates [kG]	Area [mm²]	Vdd [V]	Freq. [MHz]	Measured results for one Pairing Operation # Cycles	*Tpair* [µs]	*Ppair* [mW]	*Epair* [µJ]
Mobile Device Apple A5 32nm	-	-	-	1,000	9,909,000	9,905	-	-
HighendPC Corei7-6700K 14nm	-	-	-	4,000	840,000	210	91,000	19,110
HighendFPGA KintexUltra 20nm	14,463slice +460DSP	-	-	170	18,151	107	-	-
ASIC130nm	94	-	-	338	5,340,400	15,800	-	-
ASIC 65nm	354	2.51	-	800	512,541	640	255	163
ASIC 65nm	323	-	-	633	330,053	521	-	-
Ours: ASIC 65nm 1-core	2,793	12.8	1.33	250	8,175	33	2,850	94.0
			0.75	74.6		110	240	26.5
			0.49	9.2		792	17.2	13.7
Ours: ASIC 65nm 3-core	13,104	21.62	1.4	105	8,000	76.0	1,188	90.3
			0.75	47.6		168	68.2	11.5
			0.32	2.33		3,440	0.95	3.28
Ours: ASIC 12nm 1-core	2,300	4.0	1.17	727	8,175	**11.3**	1,013	11.5
			0.8	426		19.4	275	5.34
			0.68	272		30.3	**35.4**	**1.07**

3x～20x

6,000x ～ 20,000x

Others

Impl.	Platform	Gates [MGate]	Freq. [MHz]	Cycles	Latency [us]	Power [mW]	Energy [uJ]
Our work BLS12-381pairing	65nm CMOS/Synthesized	8.97	138	10,800	78.5	165	13.0
Our work SVDWmap				4,910	35.7		5.89
Software Impl.[6][a] BLS12-381pairing	Core i7-7700		3,600	2,340,000	650	65,000	42,300

Demonstration

We have demonstrated performance improvement and power reduction of Searchable Encryption running on Linux PC, with our Pairing Accelerator connected through PCIe
→ Demonstrated faster operation than 32-core Intel Processor

Agenda

- Background
  - ✓ Overview of Hardware Acceleration of Crypto-Algorithms, and Functionality
- Design Space Exploration of Crypto-Algorithm to Hardware
  - ✓ ECC Accelerator Design and Design space Exploration
  - ✓ Template-based Design Automation
- Introduction to d.lab, chip design platform for Japanese Academia
  - Agile-X Project ~Democratizing Chip Design~
- Conclusions

Selection of Curve

Curve	Embedded degree	Key length [bit]	Database size [bit]	Security level [bit]
BN Curve	12	224	2,688	112 → ???
		254	3,048	128 → 100~110
		256	3,072	128 → ???
		512	6,144	128
BLS Curve	12	381	4,572	128
	24	381	9,144	192
KSS Curve	18	384	6,912	192
FourQ	3.7×10^{73}	256	9.5×10^{75}	???

Flexibility for Pairing Hardware

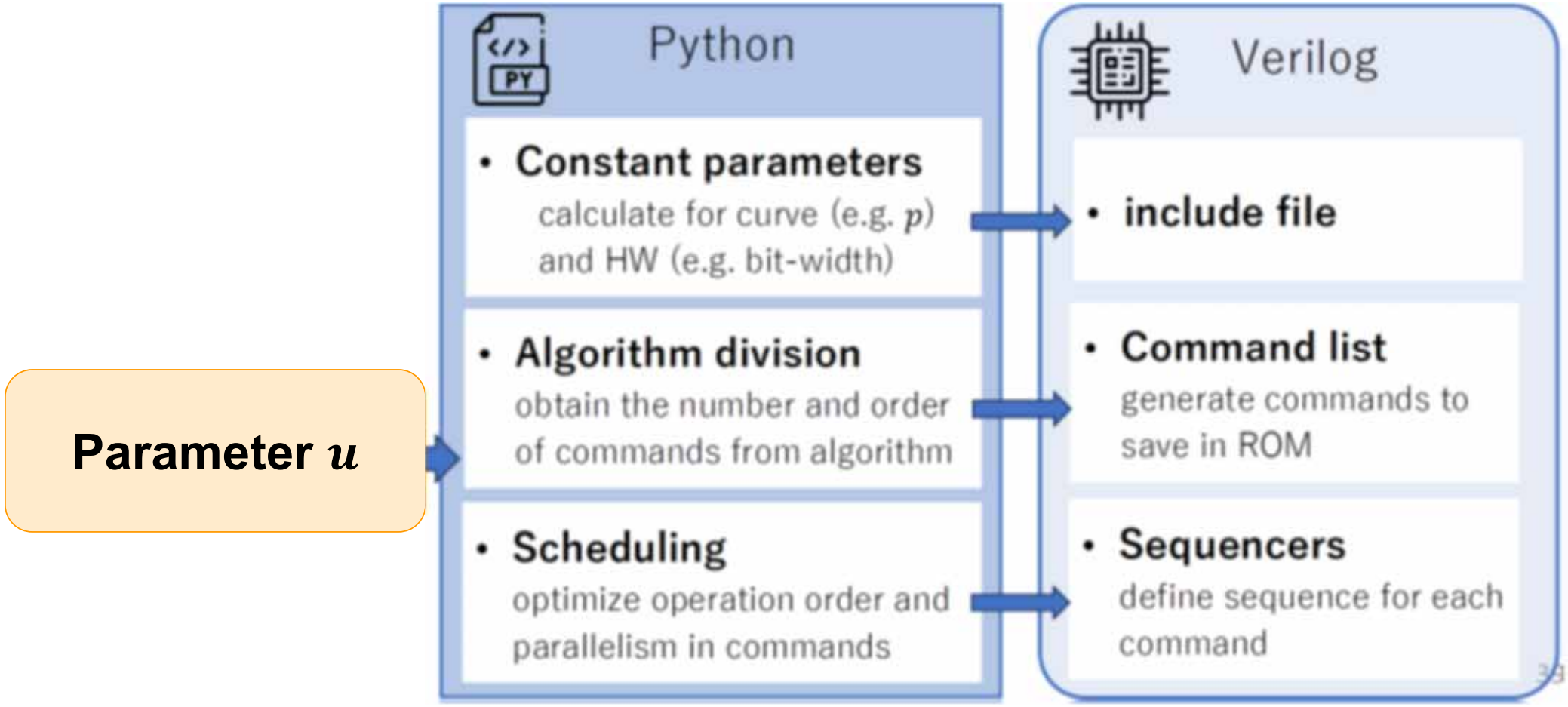
Embedding degree k, extension order of the twist-curve e, parameterized characteristics $p(u)$ and order r (u)

KSS18 curves: $k = 18, e = 3$ $p(u) = (z^8 + 5z^7 + 7z^6 + 37z^5 + 188z^4 + 259z^3 + 343z^2 + 1763z + 2401)/21, r(u) = (z^6 + 37z^3 + 343)/343$
BN curves: $k = 12, e = 2$ $p(u) = 6u^4 + 36u^3 + 24u^2 + 6u + 1, r(u) = 6u^4 + 36u^3 + 18u^2 + 6u + 1$
BLS12 curves: $k = 12, e = 2$ $p(u) = (u-1)^2(u^4 - u^2 + 1)/3 + u, r(u) = u^4 - u^2 + 1$
BLS24 curves: $k = 24, e = 4$ $p(u) = (u-1)^2(u^8 - u^4 + 1)/3 + u, r(u) = u^8 - u^4 + 1$
BLS48 curves: $k = 48, e = 8$ $p(u) = (u-1)^2(u^{16} - u^8 + 1)/3 + u, r(u) = u^{16} - u^8 + 1$

Coefficient of the curve b, twist type, parameter u, security level and Tower Extension for pairing-friendly curves

curve	b	twist type	u	security level	Tower Extension
BN254[12]	2	D	$-(2^{62} + 2^{55} + 1)$	100	$\mathbb{F}_p \xrightarrow{i^2+1} \mathbb{F}_{p^2} \xrightarrow{u^3-i-1} \mathbb{F}_{p^6} \xrightarrow{v^2-u} \mathbb{F}_{p^{12}}$
BLS12-381[13]	4	M	$-(2^{63} + 2^{62} + 2^{60} + 2^{57} + 2^{48} + 2^{16})$	117~120	$\mathbb{F}_p \xrightarrow{i^2+1} \mathbb{F}_{p^2} \xrightarrow{u^3-i-1} \mathbb{F}_{p^6} \xrightarrow{v^2-u} \mathbb{F}_{p^{12}}$
BLS12-446[14]	1	M	$-(2^{75} - 2^{73} + 2^{63} + 2^{57} + 2^{50} + 2^{17} + 1)$	132	$\mathbb{F}_p \xrightarrow{i^2+1} \mathbb{F}_{p^2} \xrightarrow{u^3-i-1} \mathbb{F}_{p^6} \xrightarrow{v^2-u} \mathbb{F}_{p^{12}}$
BLS24-315[14]	1	D	$-2^{32} + 2^{30} + 2^{21} + 2^{20} + 1$	128	$\mathbb{F}_p \xrightarrow{i^2-13} \mathbb{F}_{p^2} \xrightarrow{u^2-i} \mathbb{F}_{p^4} \xrightarrow{v^3-u} \mathbb{F}_{p^{12}} \xrightarrow{w^2-v} \mathbb{F}_{p^{24}}$
BLS24-317[14]	4	M	$2^{31} + 2^{30} + 2^{28} + 2^{27} + 2^{24} + 2^{16} + 2^{15}$	128	$\mathbb{F}_p \xrightarrow{i^2+1} \mathbb{F}_{p^2} \xrightarrow{u^2-i-1} \mathbb{F}_{p^4} \xrightarrow{v^3-u} \mathbb{F}_{p^{12}} \xrightarrow{w^2-v} \mathbb{F}_{p^{24}}$
BLS24-509[15]	1	D	$-2^{51} - 2^{28} + 2^{11} - 1$	192	$\mathbb{F}_p \xrightarrow{i^2+1} \mathbb{F}_{p^2} \xrightarrow{u^2-i-1} \mathbb{F}_{p^4} \xrightarrow{v^3-u} \mathbb{F}_{p^{12}} \xrightarrow{w^2-v} \mathbb{F}_{p^{24}}$

Template Based Design Automation



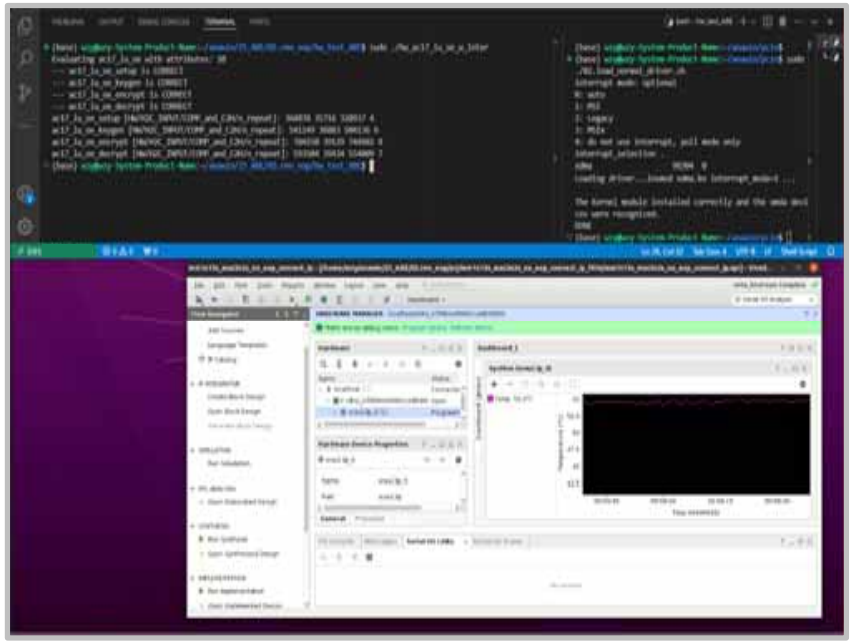
Template Based Design Automation

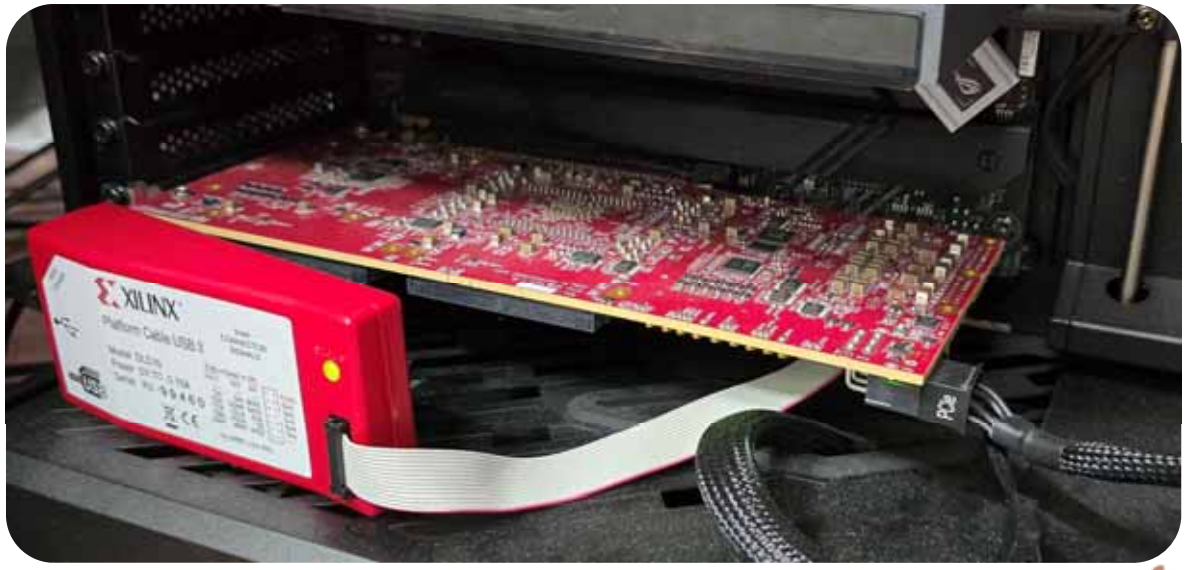
BLS12

BLS24

char. p [bit]	imple.	platform	gates [MGE]	freq. [MHz]	cycles	latency [ms]	Power [mW]	gates×latency [MGE·ms]	
								est. [9]	result
381	This work	65 nm Synthesized	5.04	137	22,873	167	62.0	1.59	0.841
	ASIC [21]	65 nm Synthesized	8.97	138	10,800	78.5	165		0.704
	SW [31]	Intel Core i7-7700	-	3,600	2,340,000	650	-		-
446	This work	65 nm Synthesized	6.43	133	27,015	203	105	2.68	1.31
	SW [32]	Intel Core i7-8550	-	1,800	2,443,808	1,358	-		-
315	This work	65 nm Synthesized	3.00 MGE	165	127,780	0.773	101.7	1.58	2.32
	SW [28]	AMD EPYC 7R32	-	2,800	4,004,000	1.43	-		-
317	This work	65 nm Synthesized	3.12 MGE	160	95,070	0.594	99.3	1.62	1.93
	SW [29]	Intel Core i9-10900X	-	3,700	22,311,000	6.03	-		-
318	FPGA [30]	Kintex-7	925 slices	200	12,960,000	64.8	-	1.63	-
509	This work	65 nm Synthesized	6.16 MGE	147	125,506	0.852	158.9	7.77	5.25
	SW [29]	Intel Core i7-6700K Skylake	-	4,000	16,807,000	4.20	-		-
518	FPGA [30]	Kintex-7	1325 slices	200	36,800,000	184	-	8.23	-

FPGA Implementation





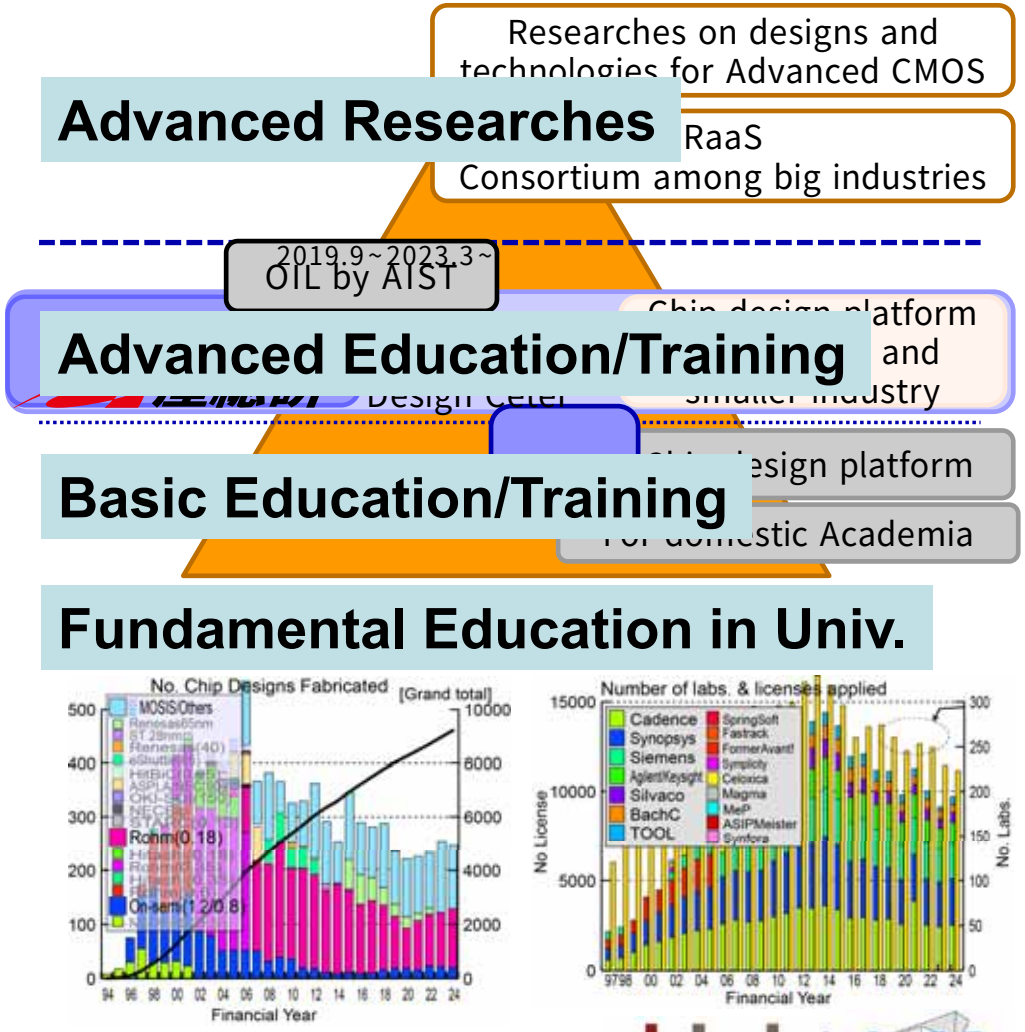
Virtex Ultrascale+
FPGA (XCVU13p-2)
on HTG930

Agenda

- Background
  - ✓ Overview of Hardware Acceleration of Crypto-Algorithms, and Functionality
- Design Space Exploration of Crypto-Algorithm to Hardware
  - ✓ ECC Accelerator Design and Design space Exploration
  - ✓ Template-based Design Automation
- Introduction to d.lab, chip design platform for Japanese Academia
  - Agile-X Project ~Democratizing Chip Design~
- Conclusions

d.lab / VDEC related activities in U. Tokyo

- **Chip design platform among Japanese Universities**
  - VDEC activities(1996.5~now), now as a part of d.lab activities: Chip fabrication gateway, EDA tools, and chip design education for Academia
  - EDA tool training, Design flow training, etc.
- **AI Chip design Center**
  - Joint activity by d.lab & AIST, supported by NEDO and METI (2018.8~2023.3, and now continue in mostly self-support)
  - Provide design environment for startup and smaller industries in Japan
- **d.lab (2019.10) / RaaS activities**
  - Consortium by larger industry for the state-of-the art chip design with the advanced process node
- **Agile-X project (2022.4~2032.3)**
  - MEXT project on X-nics
- **Semiconductor education initiatives in UT**
  - Chip design hackathon (2023.4~)
  - University-wide Education Program on Semiconductor (2024.4~)
  - TSMC-UTokyo lab (2025.4~): TSMC ADFP-N16 Education,etc
- **METI-NEDO "Advanced SoC Design Talent Incubation Program (ADIP) (2024.11~)**



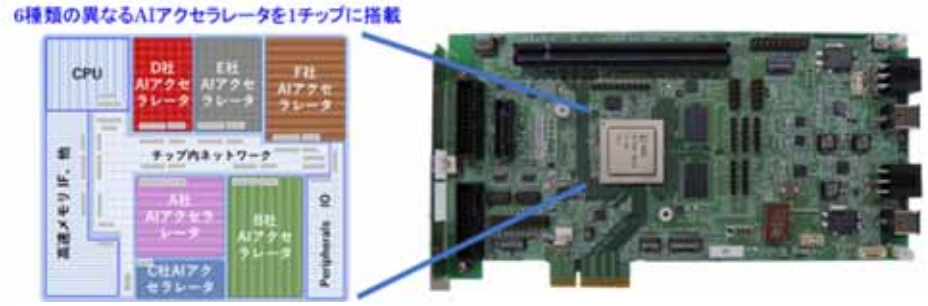
AIDC Activities and SoC Design/Education

AI-One

・TSMC 28nm
・Synopsys IPs
・6 AI-IPs from 6 companies
・June '21 Wafer out, Nov. '21 PKG, Jan. '22 Board

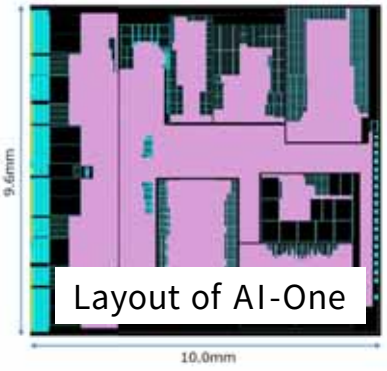
AI-Two

・TSMC 12nm
・Synopsys IPs
・3 AI-IPs from 3 companies
・Nov.'22 Wafer out, Jan.'23 Board, March'23 Demo



Floorplan of AI-One

Evaluation board of AI-One



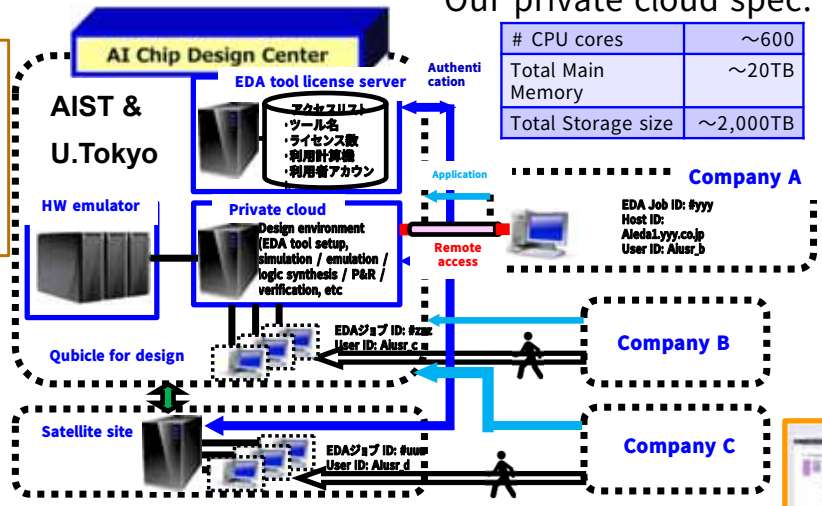
Layout of AI-One

GDS size	10.0mm x 9.6mm
Die size	9.0mm x 8.64mm

https://www.nedo.go.jp/news/press/AA5_101427.html

Our private cloud spec.

# CPU cores	～600
Total Main Memory	～20TB
Total Storage size	～2,000TB

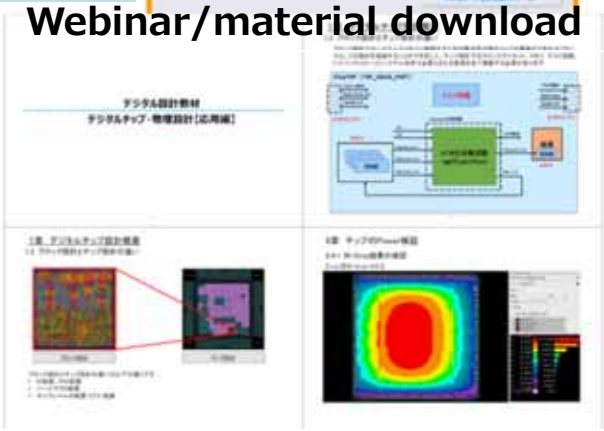


SoC Design hands-on training

~ 6-month: from HLS to Physical implementation and Software design

Verification speedup by Hardware emulator

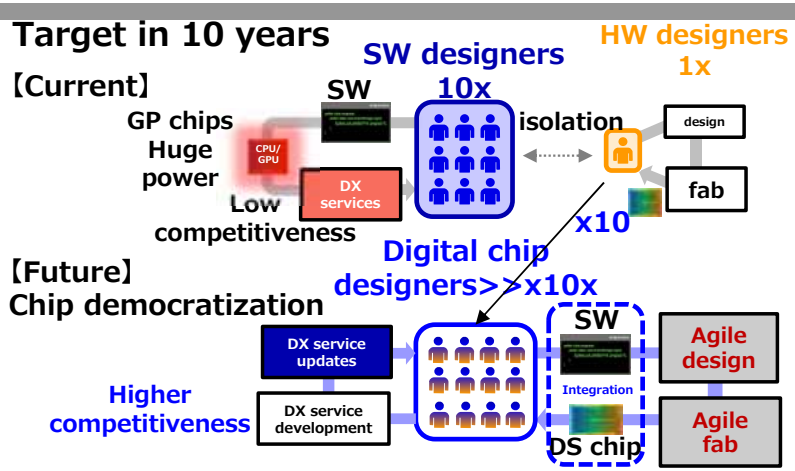
Webinar/material download



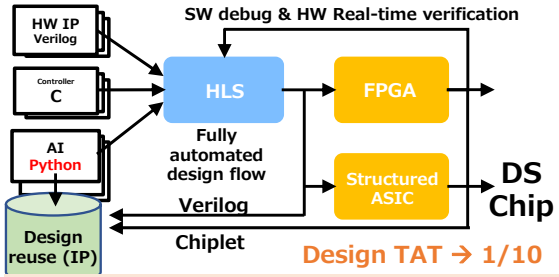
東京大学 THE UNIVERSITY OF TOKYO

Agile-X ~Innovative Semiconductor Technology Platform for Chip Democratization~

Target in 10 years



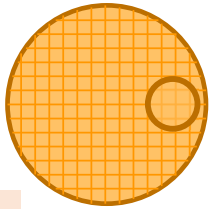
Agile Design platform



Higher level description language (e.g. Python) based design for 10x design efficiency and 100x performance than CPU

Agile Fabrication platform

Structured ASIC wafer :
MOS + local metals
6′ ~12′ wafer



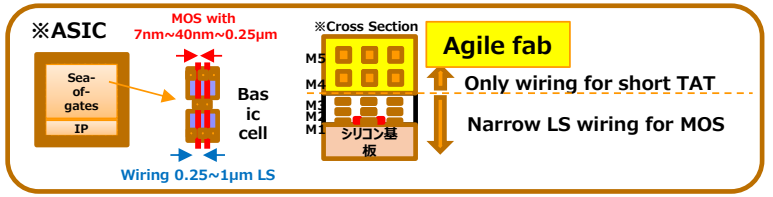
Mask-less Super CR fab
0.25μm LS wiring by 3-day
Over 40nm~65nm CMOS

0.1μm Class Agile LSI
100M Gate
>3ML Al/Cu

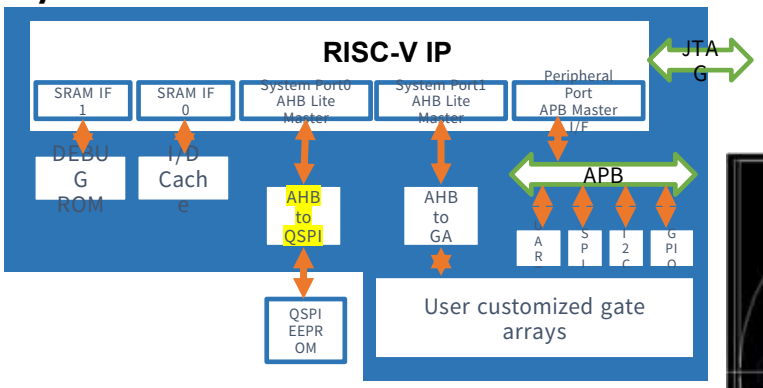
dicing

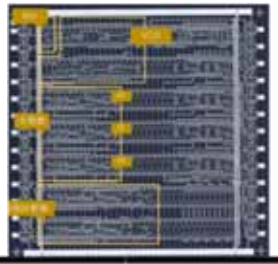
Mask-less local CR fab
~1μm LS wiring by 1-day
Over 0.13μm~0.25μm CMOS

0.25μm Class Agile LSI
10M Gate
2ML Al

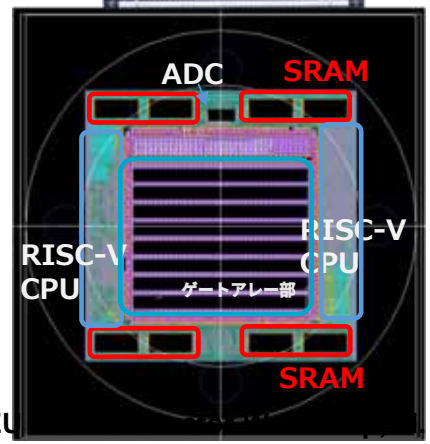


System Architecture

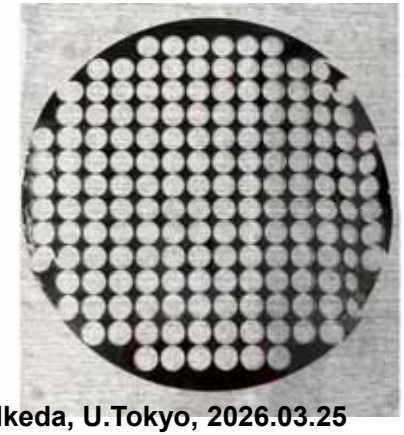




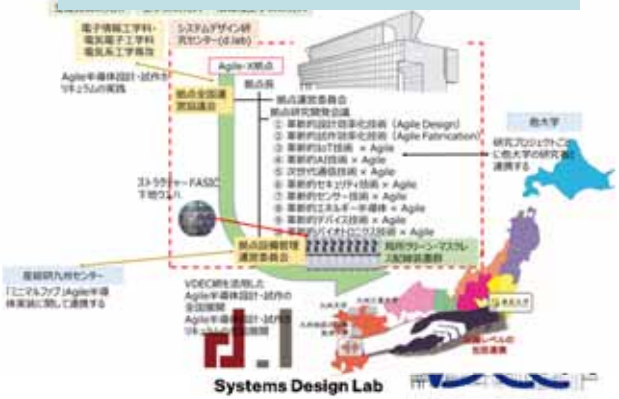
One Metal Layer GA:
Design: 5-day,
Process: 1-day,
Measurements: 4-day：
Undergrad. Experimental course: since 1996



Layout

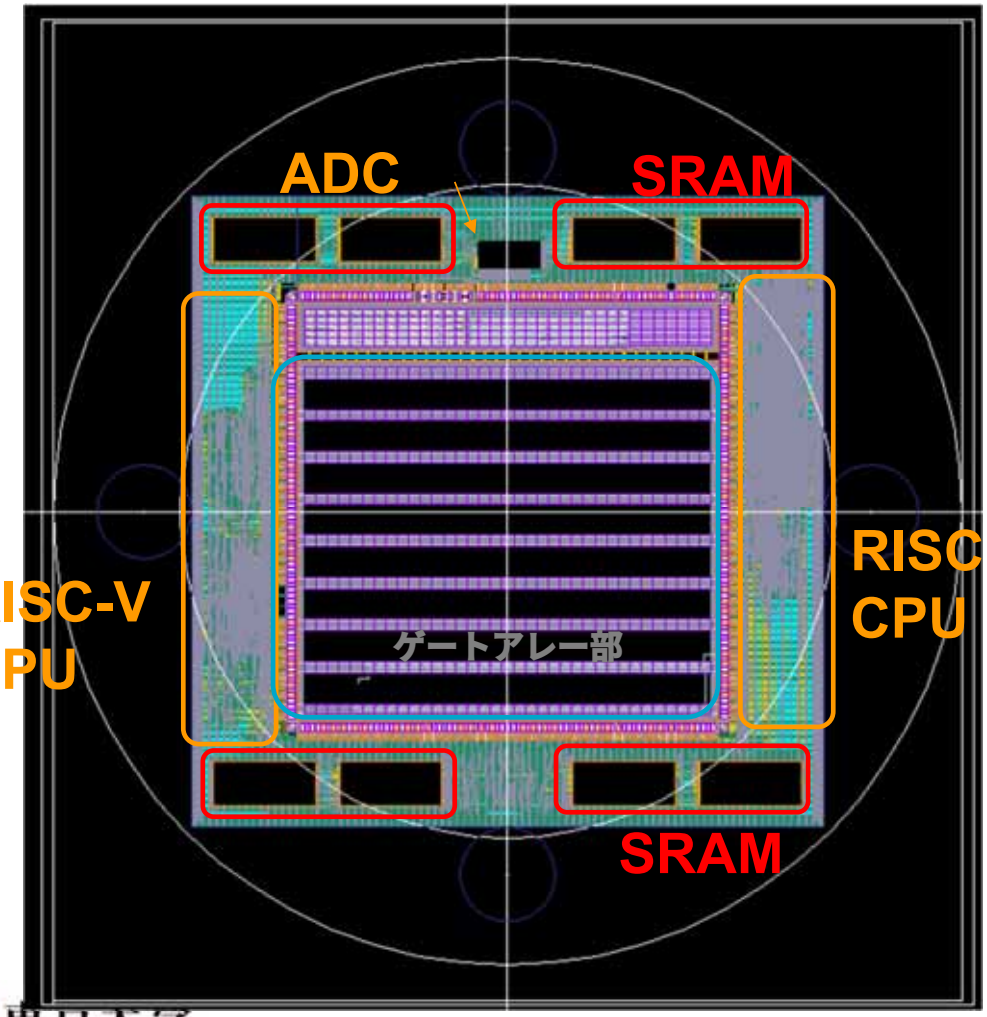


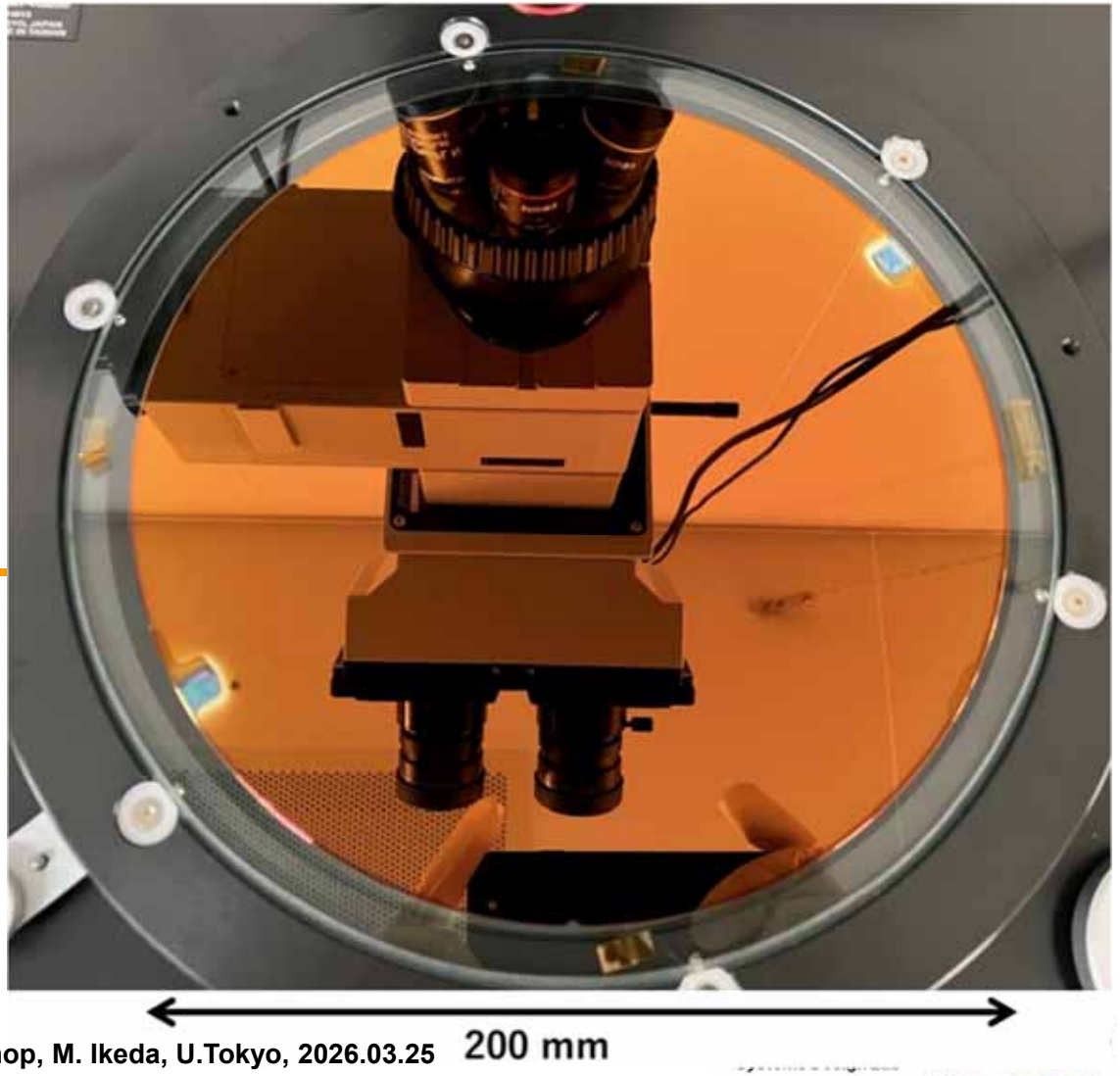
From d.lab → EE department → Intra-U.Tokyo → Among Japanese Academia



東京大学 THE UNIVERSITY OF TOKYO

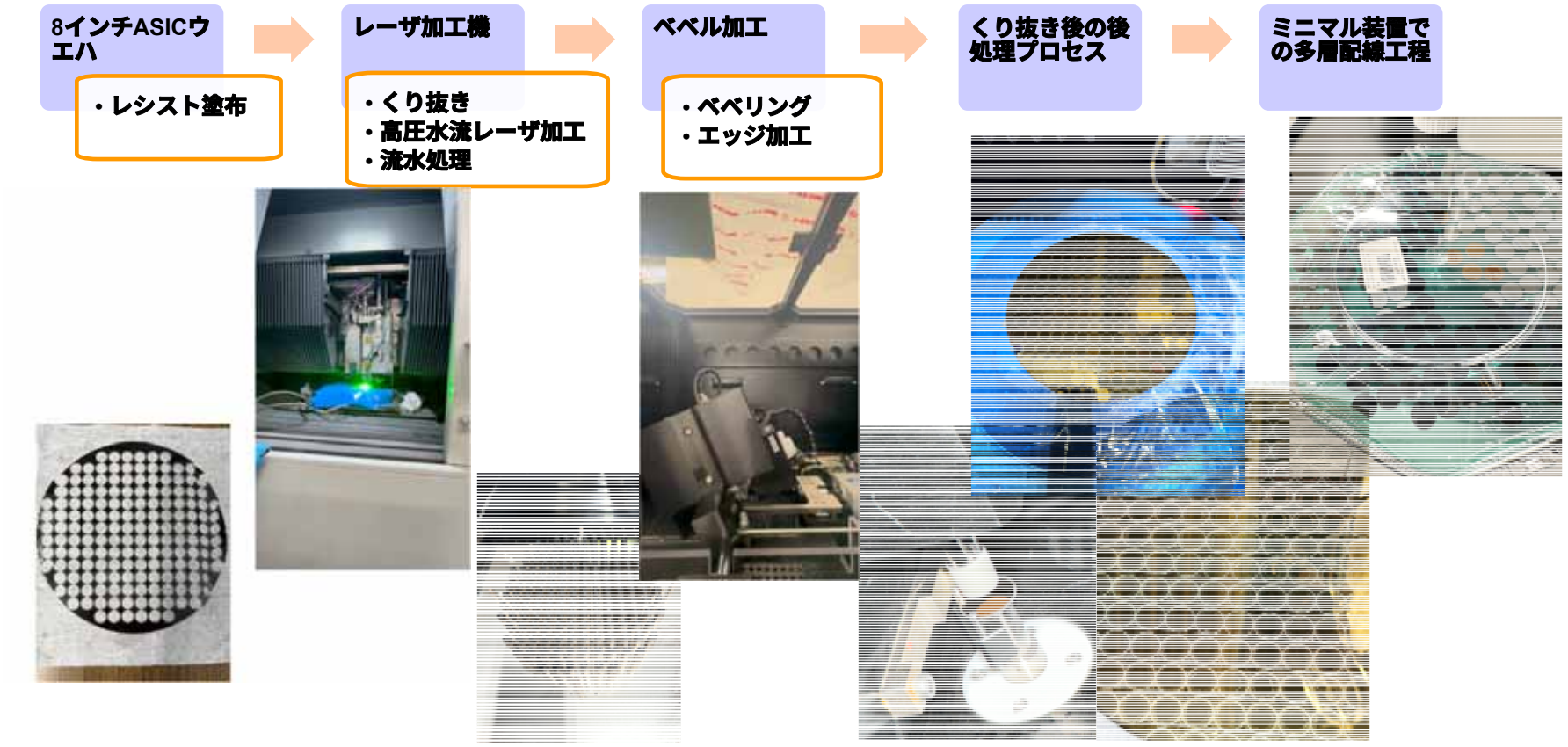
Japan-EU


ADC
SRAM
RISC-V CPU
RISC-V CPU
ゲートアレー部
SRAM

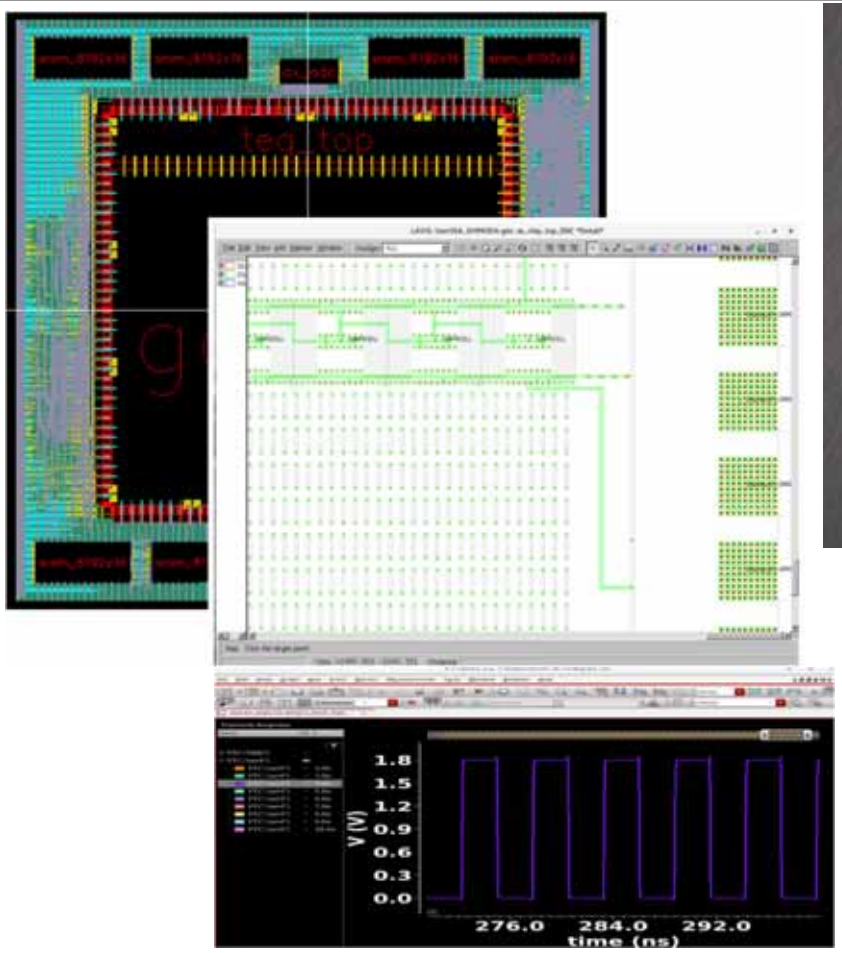

200 mm

Agile-X 2-ML Process

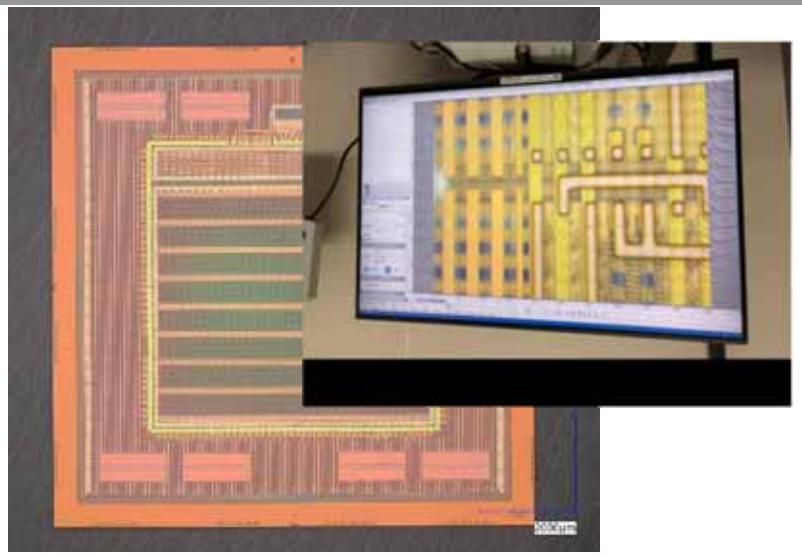
8-inch wafer to 0.5-inch wafer

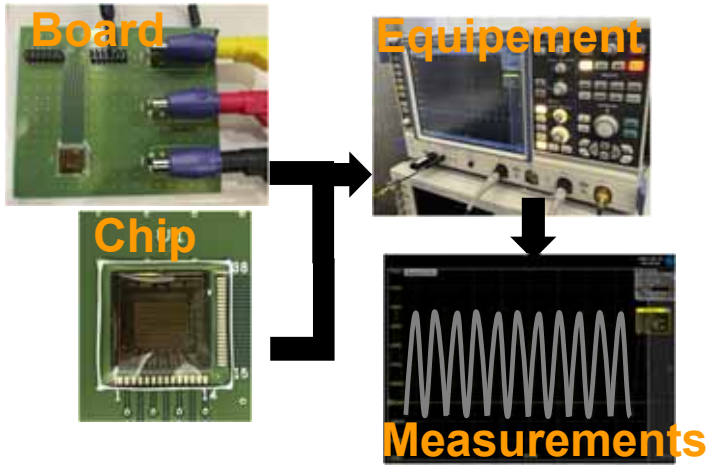


Trial for Experiment Course



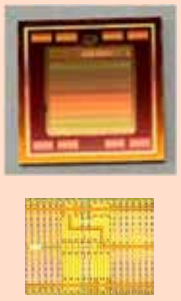
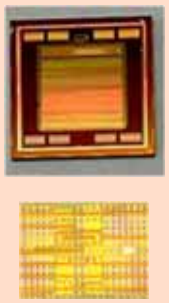
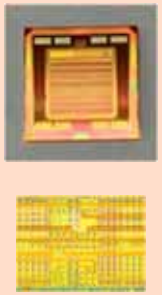
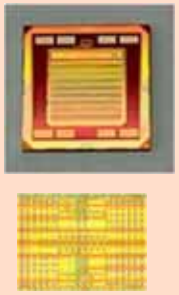
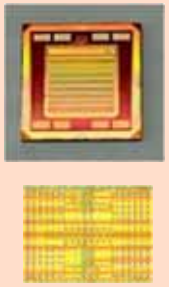
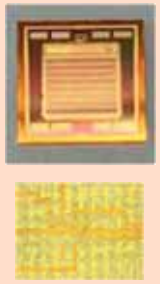
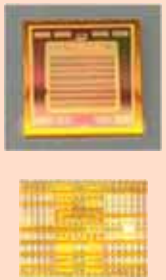
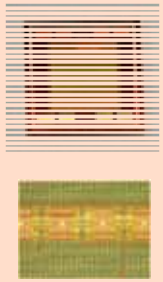
Design Env.: Layout/Sim.





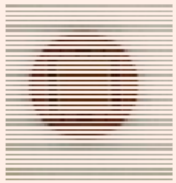
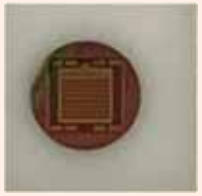
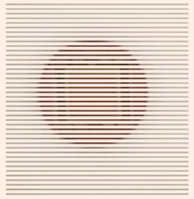
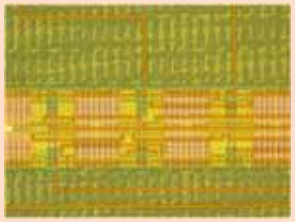
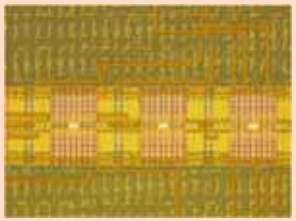
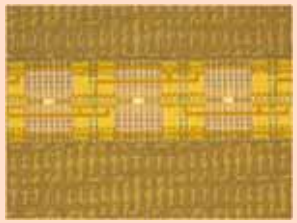
Access to chip from PC through USB

Chips designed and fabricated..1

Ring Osc. (1)	Shift Regist.	Ring Osc. (2): 学生実習		Shift Regist. (2)	
					
ADD4 (1)	**ADD4 (2)**	**Via Short Cir**	**PWM[*1]**	**LFSR[*2]**	**VCO[*3]**
					

*[1]PWM: Pulse Width Modulation
*[2]Linear Feedback Shift Register
*[3]VCO: Voltage-Controlled Oscillator

Chips designed and fabricated..2

学生実習 (2025/11/7)			
Pulse Wave Modulation	Dice	Ring Oscillator	Ring Oscillator
			
			

Conclusions

- We have been working for hardware accelerator designs of crypto-algorithms…including:
  - Design space exploration of crypto-algorithms, based on Elliptic Curve, Pairing, etc..
  - Template-based design automation for Pairing Algorithms
  - Design optimizations for functional crypto-algorithms including ABE
  - PQC
- d.lab, former VDEC, has been the only one entity providing chip design platform for entire Japanese academia, also AIDC for smaller industries
  - Agile-X project for short TAT chip design and fabrication platform to democratize chip design