



2023第一季法人說明會

May 10th, 2023

Embedded Wisely, Embedded Widely

ememory



智慧財產權聲明

All rights, titles and interests contained in this information, texts, images, figures, tables or other files herein, including, but not limited to, its ownership and the intellectual property rights, are reserved to eMemory. This information may contain privileged and confidential information. Some contents in this information can be found in Logic Non-Volatile Memory (The NVM solutions from eMemory), published in 2014. Any and all information provided herein shall not be disclosed, copied, distributed, reproduced or used in whole or in part without prior written permission of eMemory Technology Inc.

eMemory, NeoBit, NeoFuse, NeoEE, NeoMTP, NeoROM, EcoBit and NeoPUF are all trademarks and/or service marks of eMemory in Taiwan and/or in other countries.



投資安全聲明

This presentation contains forward-looking statements, which are subject to risk factors associated with semiconductor and intellectual property business. It is believed that the expectations reflected in these statements are reasonable. But they may be affected by a variety of variables, many of which are beyond our control. These variables could cause actual results or trends to differ materially which include, but are not limited to: wafer price fluctuation, actual demand, rapid technology change, delays or failures of customers' tape-outs into wafer production, our ability to negotiate, monitor and enforce agreements for the determination and payment of royalties, any bug or fault in our technology which leads to significant damage to our technology and reputation, actual or potential litigation, semiconductor industry cycle and general economic conditions. Except as required by law, eMemory undertakes no obligation to update or revise any forward-looking statements, whether as a result of new information, future events, or otherwise.



Contents

- 1 營運回顧
- 2 未來展望
- 3 **How PUF-based Solutions Secure ChatGPT and AI**
- 4 Q&A
- 5 附錄



營運回顧

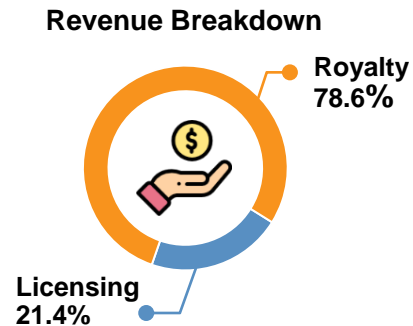
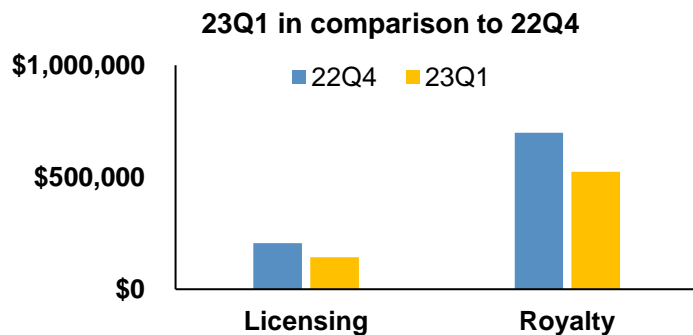
第一季綜合損益表

(thousands of NT dollars)

	Q1 2023	Q4 2022	QoQ	Q1 2022	YoY
Revenue	667,751	902,704	-26.0%	727,107	-8.2%
Gross Margin	100%	100%	-	100%	-
Operating Expenses	300,657	368,090	-18.3%	313,846	-4.2%
Operating Income	367,094	534,614	-31.3%	413,261	-11.2%
Operating Margin	55.0%	59.2%	-4.2 pts	56.8%	-1.8 pts
*Net Income	313,090	430,536	-27.3%	366,019	-14.5%
Net Margin	46.1%	47.6%	-1.5 pts	49.8%	-3.7 pts
EPS (NT\$)	4.20	5.77	-27.2%	4.91	-14.5%
ROE	38.9%	62.2%	-23.3 pts	55.0%	-16.1 pts

*Net income attributable to Shareholders of the Company

第一季營收貢獻分析



Revenue

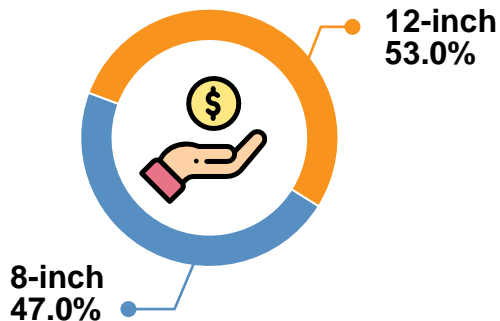
NT\$ Thousands	Q1 2023	Q4 2022	Change (QoQ)	Q1 2022	Change (YoY)
Licensing	143,049	205,104	-30.3%	191,608	-25.3%
Royalty	524,702	697,600	-24.8%	535,499	-2.0%
Total	667,751	902,704	-26.0%	727,107	-8.2%

第一季營收分析 – 產品線

Technology	Q1 2023								
	Total Revenue			Licensing Revenue			Royalty Revenue		
	% of Q1 Revenue	Change (QoQ)	Change (YoY)	% of Q1 Licensing	Change (QoQ)	Change (YoY)	% of Q1 Royalty	Change (QoQ)	Change (YoY)
NeoBit	28.2%	-30.0%	-22.7%	19.7%	-22.6%	-19.8%	30.5%	-31.1%	-23.2%
NeoFuse	63.9%	-22.4%	-0.8%	49.6%	-28.5%	-42.9%	67.8%	-21.0%	16.3%
PUF-Based	2.5%	-63.6%	126.6%	11.5%	-60.7%	138.2%	0.0%	-93.8%	-46.3%
MTP	5.4%	-5.6%	-21.7%	19.2%	0.0%	8.4%	1.7%	-19.8%	-58.2%

第一季營收分析 – Wafer Size

Q1 Royalty Breakdown



- 8-inch wafers contributed 47% of royalty, down 25.5% sequentially and down 9.2% yearly.
- 12-inch wafers contributed 53% of royalty, down 24.1% QoQ but up 5.3% YoY.

Wafer Size	Q1 2023		
	% of Q1	Change (QoQ)	Change (YoY)
8-Inch	47.0%	-25.5%	-9.2%
12-Inch	53.0%	-24.1%	5.3%



未來展望

未來展望

Licensing & Royalty:

- Licensing will significantly grow during the rest of the year, driven by PUF-based security solutions.
- With more than 1000 new products tape out in the pipeline, royalty will regain growth momentum as new tape outs move into production.

New IP Technology & Business Development:

- This year, PUF-based solutions will be adopted in 5/6/7nm CPU, DPU, AI and Automotive-related applications.
- Continue working with foundries to develop NeoFlash to increase the penetration rate of mature processes.
- Continue developing PUF-based security solutions in the most advanced processes with CPU partners.



How PUF-based Solutions Secure ChatGPT and AI

Asking ChatGPT about Security.

MI

How do you secure ChatGPT



As an AI language model, ChatGPT is secured through various measures that are designed to ensure the confidentiality, integrity, and availability of the system. Here are some of the ways ChatGPT is secured:



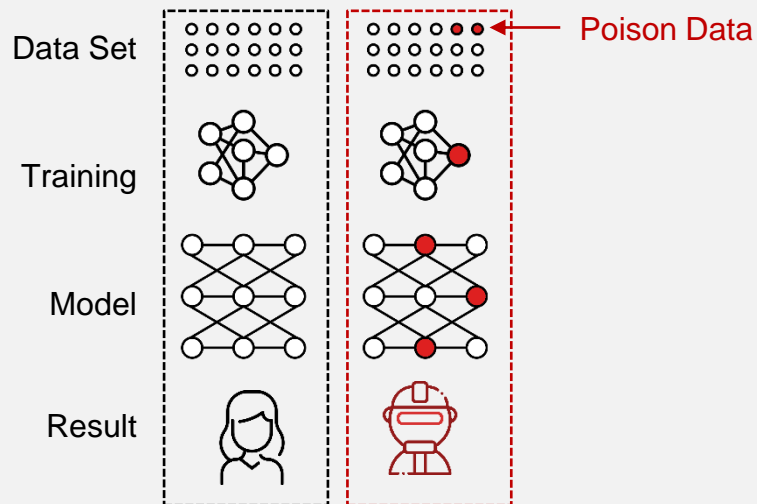
1. **Data Encryption:** All the data exchanged between the user and ChatGPT is encrypted using **industry-standard encryption protocols**. This helps to protect the data from unauthorized access or interception.
2. **Access Control:** Access to ChatGPT is restricted to authorized personnel only. **Authentication mechanisms such as username and password** are used to ensure that only authorized users can access the system.
3. **Auditing and Logging:** ChatGPT logs all user activities and interactions, including user inputs and system outputs. This helps to **identify and investigate any security incidents or breaches**.
4. **Regular Updates:** ChatGPT is regularly updated with the latest **security patches and fixes**. This helps to mitigate any known security vulnerabilities and keep the system secure.
5. **Training and Awareness:** All personnel involved in the operation and maintenance of ChatGPT undergo regular **security awareness training** to help them identify and mitigate potential security threats.

Use PUF-based Security	
1	Key generation for encryption
2	Unique Identity (UID) and Secret Key generation for authentication
3	ID generation for users
4	Secure over-the-air (OTA) firmware/software updates through signature verification
5	Mitigate human errors by hardware security

Major Attacks in AI

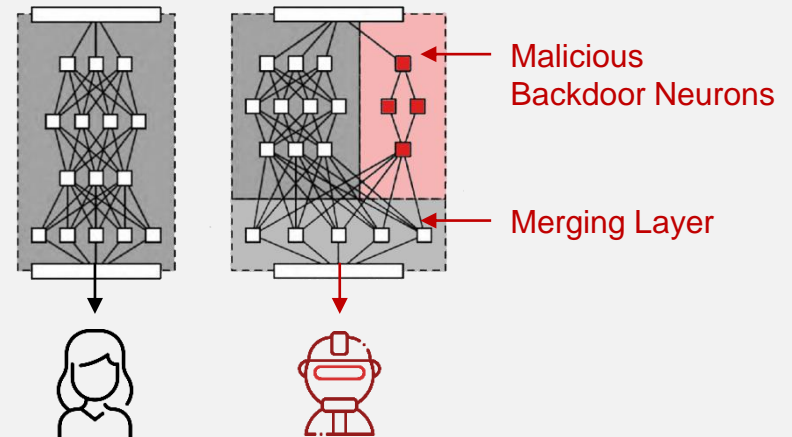
Poisoning Attack

Poisoned training data leads to a poisoned model



Backdoor Attack

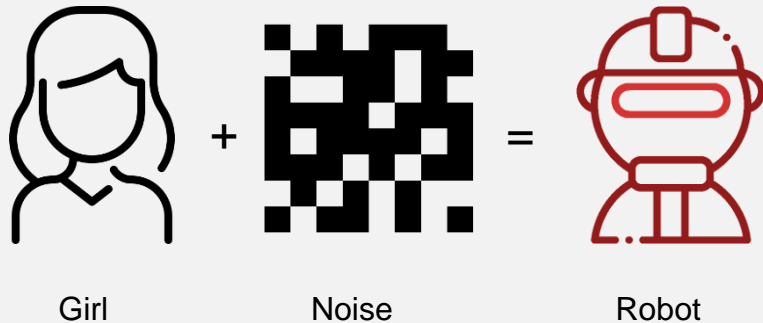
A replaced model gives incorrect output



Major Attacks in AI cont. ■

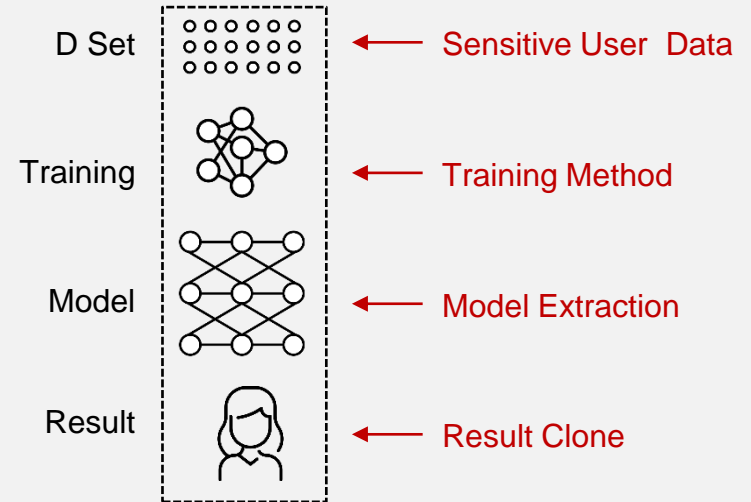
Evasion Attack

AI model mis-performs due to **modified Input Data or Inference Results**



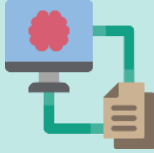

Stealing Attack

Hacker **steals AI know-how** including data, model parameters, or sensitive information





How to Prevent Attacks on AI .

- Each of these types of attacks requires different protection methods
- PUF-based security co-processor, PUFcc, can well protect AI systems

Types of Attacks	Problems	Solution
 Poisoning Attack	Training data may be corrupted	<ul style="list-style-type: none">• Signing the training data
 Backdoor Attack	Model may be modified, replaced, or even stolen by attackers	<ul style="list-style-type: none">• Signing the model• Encryption and Key management

How to Prevent Attacks on AI cont. ■

- Each of these types of attacks requires different protection methods
- PUF-based security co-processor, PUFcc, can well protect AI systems

Types of Attacks	Problems	Security Solution
 Evasion Attack	Attacker can tamper input data to wreck the model, or tamper with the inference result	<ul style="list-style-type: none">• Authenticate and provision users (UID)• Encryption and Key management
 Stealing Attack	Hardware implementations of AI are prone to hacking and theft, including training data, model and inference result	<ul style="list-style-type: none">• Authenticate provision users (UID)• Signing model/data• Encryption and Key management• Anti-tamper hardware design

Securing AI with PUF-based Solutions ■

- PUF-based IPs provide comprehensive protection to safeguard AI applications

Best in-class Root of Trust



- Secure OTP Qualified Worldwide
- High performance TRNG
- High quality on-chip PUF fingerprint
- Controller and flexible interfacing

Complete set of Cryptographic Engines



- Symmetric ciphers (AES)
- Public Key cryptography (RSA/ECC)
- Secure hashing (SHA-2)
- Key wrapping and derivation

Certified Anti-tampering Designs



- Data/address scrambling
- Output data fault detection
- Side-channel attack countermeasures

Advanced Security Protocols and Applications



- Secure boot
- Transport Layer Security (TLS) Protocol
- Key management
- Anti-cloning and asset protection



Q&A



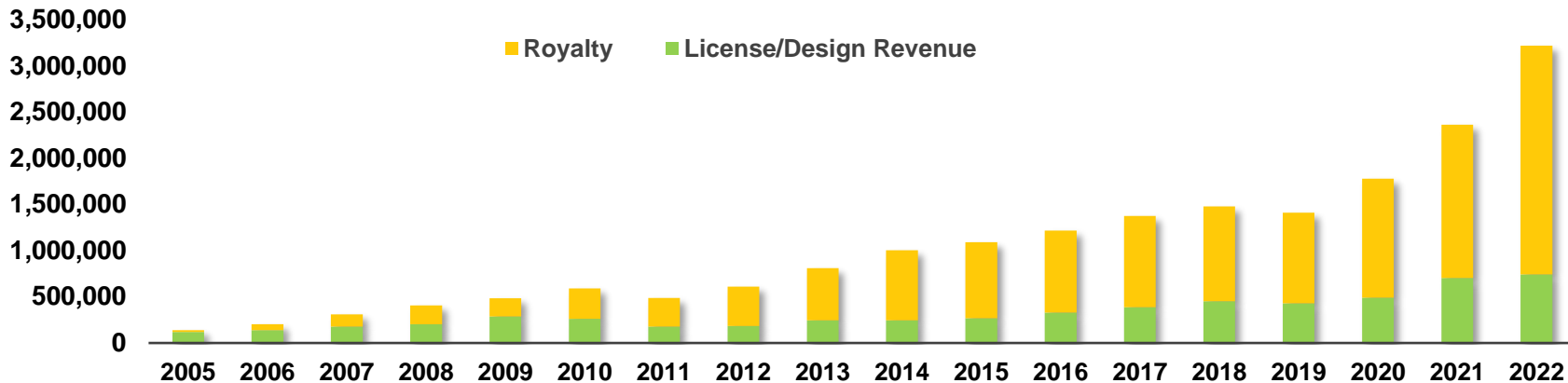
附錄

公司介紹

- eMemory is the global leader of embedded non-volatile memory IP

Revenue Trend

(Unit: NT\$ 1,000)



Founded
In 2000

Based in Hsinchu, Taiwan.
IPO in 2011. Over 50M wafers shipped.

1100+
Patents Issued

199 pending patents. 334 employees with 67% R&D personnel.

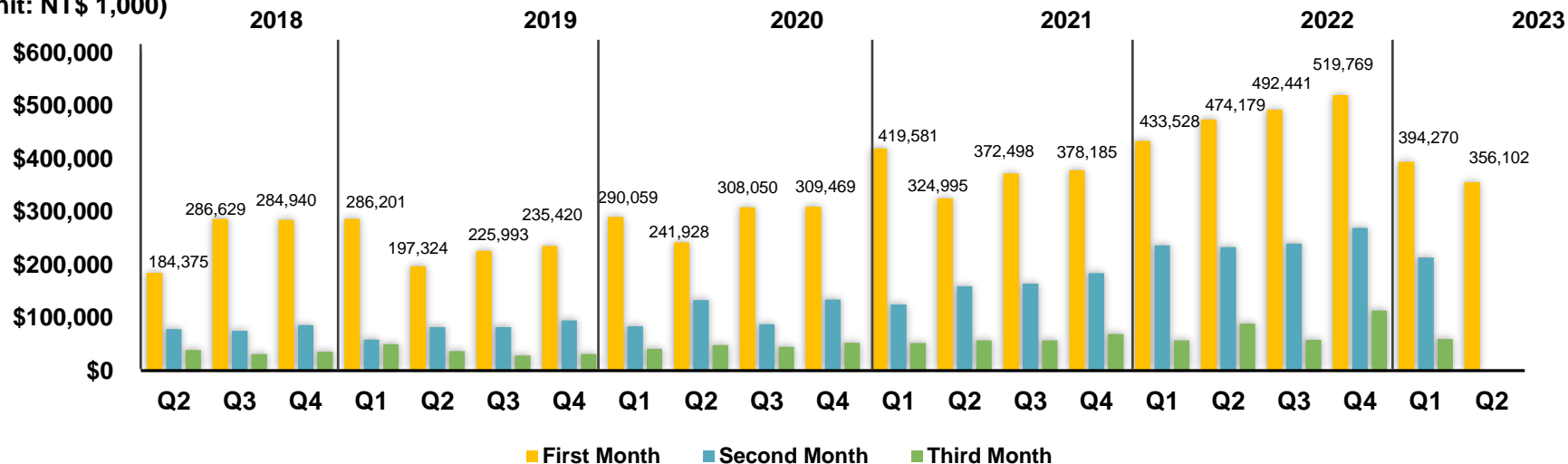
Best IP Partner
With TSMC

TSMC Best IP Partner Award since 2010.

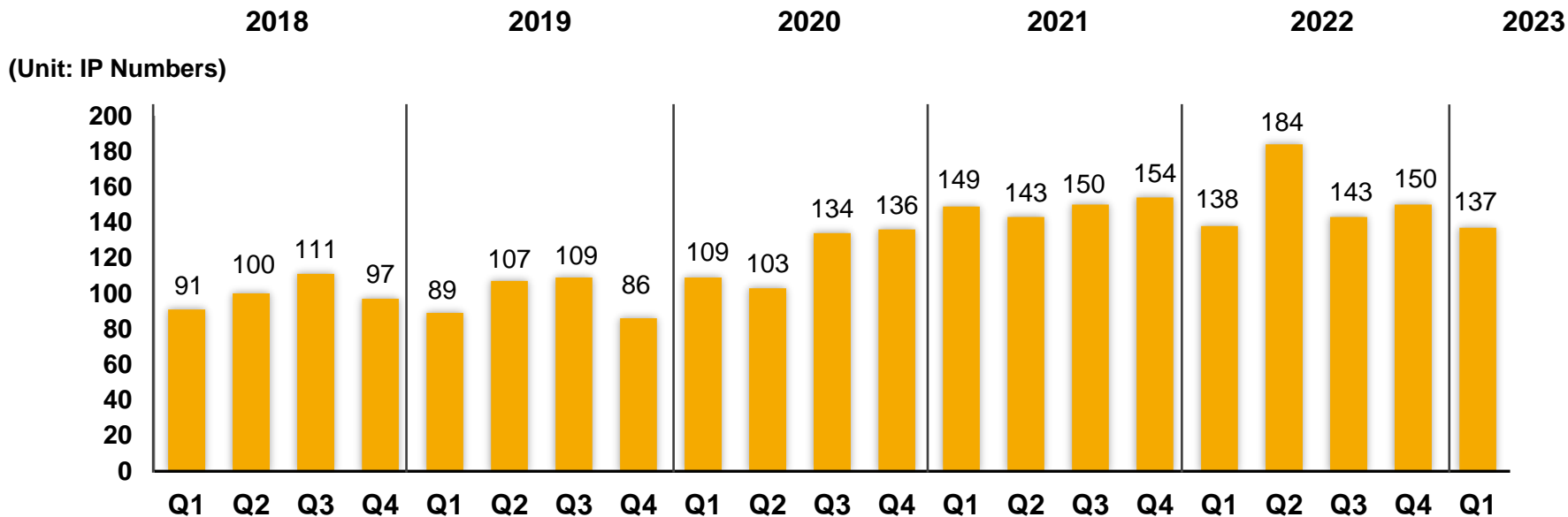
每季營收

- 1st month: Receive License Fees of the month and Royalty from most foundries on previous quarter's wafer shipments.
- 2nd month: Receive License Fees of the month and Royalty from other foundries.
- 3rd month: License Fees Only.

(Unit: NT\$ 1,000)



每季新Tape-out (NTO)



全球客戶

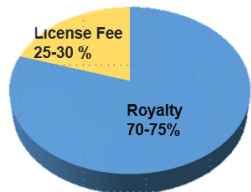
- Our IP solutions are adopted by leading foundries, IDMs and fables worldwide

Country	Foundry	IDM	Fabless
Taiwan	4	1	323
China	9	0	1105
Korea	4	0	96
Japan	4	7	80
North America	1	1	365
Europe	2	1	211
Others	1	0	103



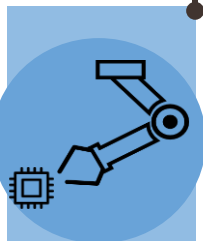
營運模式

- Recurring royalty is the backbone of our business



- 70-75% revenue are from royalty based on wafer production
- More adoption = more volume shipment
- More advanced node wafers = higher ASP per wafer

Revenue Breakdown



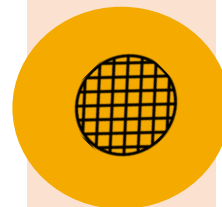
License Fee
Foundries Process
Development

1-4 years



Design License Fee
Fabless Product
Development

1-4 years



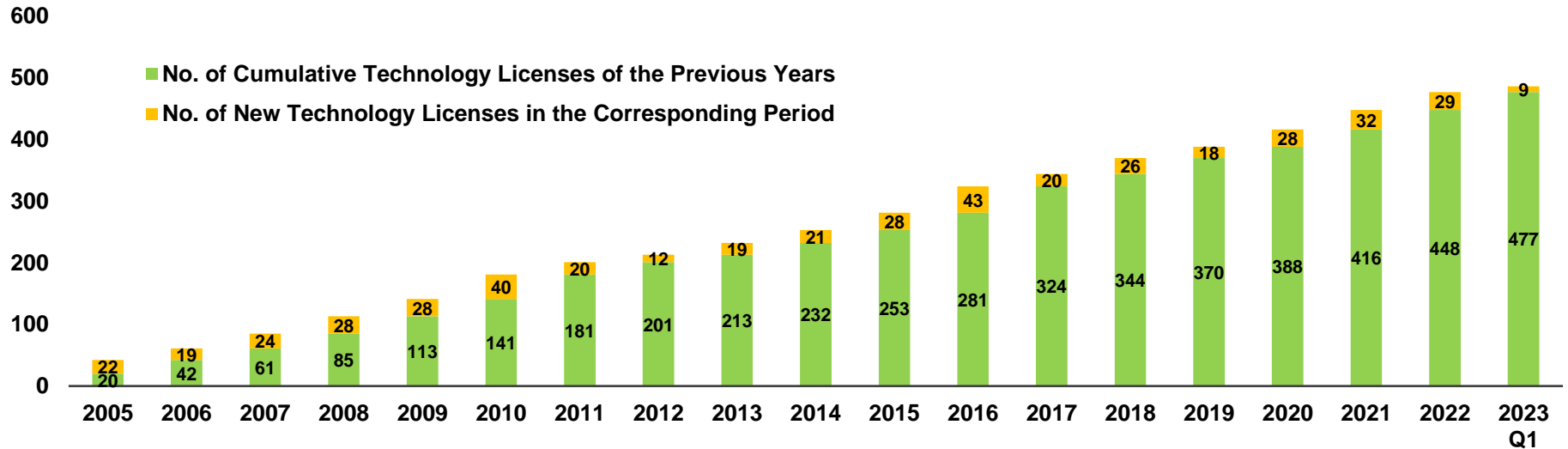
Royalty
Wafer Mass Production

技術授權合約

Number of Licenses

Year	2016	2017	2018	2019	2020	2021	2022	2023 Q1
License	43	20	26	18	28	32	29	9

Note: Terms (including number of process platforms and licensing fees) for each technology license are set contractually. Payments are made according to set milestones, and there are no particular seasonal factors involved.



建構中的技術製程平台

- New technologies are being developed for 140 platforms by Q1 2023.
- 9 licensing contracts were signed.

Technology	3nm	4/5nm	6/7nm	12/16nm	22/28nm	40nm	55/65nm	80/90nm	0.11~ 0.13um	0.15~ 0.18um	>0.25um
NeoBit	-	-	-	-	-	-	2	1	14	11	1
NeoFuse	2	2	1	7	11	6	17	7	2	3	-
PUF-Based	-	2	-	-	1	-	1	-	-	-	-
MTP	-	-	-	-	2	1	8	7	13	18	-

Note: As of March 31st, 2023

建構中的技術製程平台

- Developments by process nodes

12" Fabs	Production	Development	IP Type	Process Type
3nm	0	2	OTP	FF
4/5nm	2	4	OTP, PUF	FF
6/7nm	4	1	OTP, PUF	FF, FF+
12/16nm	8	7	OTP, PUF	FF, FF+, FFC, FFC+, LPP, DRAM
22/28nm	44	14	OTP, PUF, MTP	LP/ULP/ULL, HPC/HPC+, HV-OLED, DRAM, SOI, ReRAM, MRAM, E-Flash, BCD
40nm	22	7	OTP, PUF, MTP	LP/ULP, E-Flash, HV-DDI/OLED, ReRAM
55/65nm	38	28	OTP, PUF, MTP	LP/ULP, E-Flash, HV-DDI/OLED, DRAM, CIS, BCD, PM
80/90nm	23	12	OTP, MTP	HV-DDI/OLED, LP, Generic, BCD, CIS
0.11/0.13um	20	3	OTP, MTP	HV-DDI, BCD, Generic
0.15/0.18um	2	11	OTP, MTP	BCD, Generic
Total	163	89		

8" Fabs	Production	Development	IP Type	Process Type
80/90nm	9	3	OTP	HV-DDI, LL, BCD
0.11/0.13um	76	26	OTP, MTP, PUF	HV/HV-MR, BCD, LP/LL, CIS, Green, Flash, SOI, Generic
0.152/0.16/0.18um	225	21	OTP, MTP	HV/HV-MR, BCD, LP/LL, CIS, Green, Generic
0.25um	42	1	OTP	BCD
0.3/0.35um	53	0	OTP, MTP	UHV, BCD
0.4/0.5um	11	0	OTP	UHV, BCD
Total	416	51		

Note: As of March 31st, 2023

A hand is shown dropping a coin into a stack of coins. A small green plant with three leaves is growing out of the stack. The background is a warm, golden-brown color with a white brushstroke effect on the left side.

THANKS

Embedded Wisely, Embedded Widely

For more information, please visit:

eMemory Website: <https://www.ememory.com.tw/>

PUFsecurity Website: <https://www.pufsecurity.com/>