Research Activities in KDDI Research on Post-Quantum Cryptography

Shintaro Narisada, Kazuhide Fukushima, Shinsaku Kiyomoto

KDDI Research, Inc.

29, November 2023

Topics:
1. Security Evaluation of **Code-based Cryptography** — Activities in DecodingChallenge — (15min)
2. Ultra High-Speed **Symmetric Cryptography**: Rocca-S (5min)

Tomorrow, Together KDDI

おもしろいほうの未来へ。 au

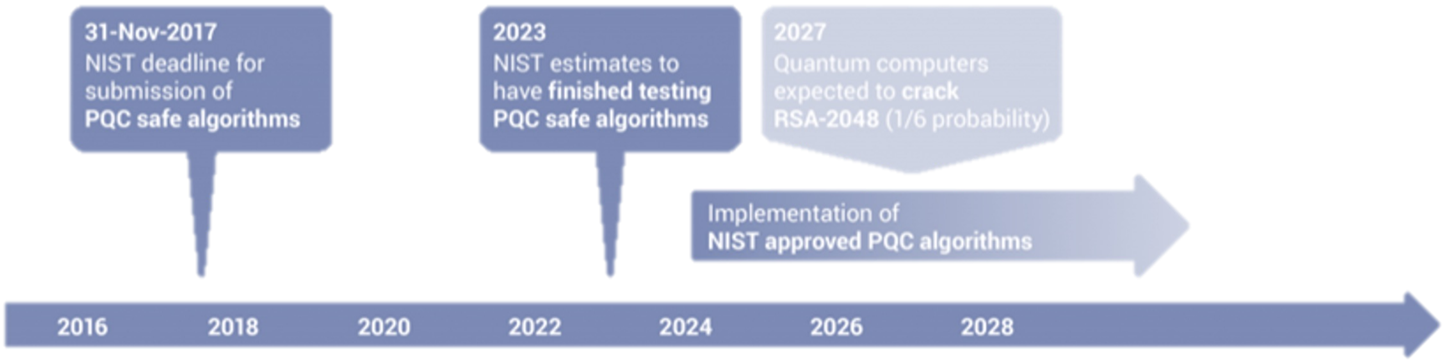
Security Evaluation of Code-based Cryptography

— Activities in DecodingChallenge —

NIST-PQC

- In 2016, the National Institute of Standards and Technology (NIST) launched NIST-PQC project to select the U.S. standard for **post-quantum cryptography**.
  - They accepted 69 submissions.
- NIST evaluated algorithms across three categories: **public-key encryption** (merged with key-establishment in Round 2), **key-establishment** and **digital signature**.
- The objective is to finalize the selection of the U.S. standard by around 2024.
  - Digital signatures are important considering the requirement for long-term security preservation.

National Institute of Standards and Technology
U.S. Department of Commerce



Latest Trends in NIST-PQC

- On July 5, 2022, NIST-PQC announced that four schemes were selected as the candidates of the US standard.
- Additional four schemes are currently undergoing evaluation in Round 4.

(light blue) : Selected (light orange) : Round 4

Lattice-based		Code-based		Isogeny-based	Hash-based
CRYSTALS-KYBER (Key-Est)	CRYSTALS-DILITHIUM (Key-Est)	Classic McEliece (Key-Est)	BIKE (Key-Est)	SIKE (Key-Est) **Attacked**	SPHINCS+ (Sign)
FALCON (Sign)		HQC (Key-Est)			

- The remaining code-based cryptographic schemes in Round 4 are attracting attention as candidates.

"Although Classic McEliece is widely regarded as secure, NIST does not anticipate it being widely used due to its large public key size. **NIST may choose to standardize Classic McEliece** at the end of the fourth round." NIST PQC Forum July 6, 2022

Cryptographic Competition

- We evaluate the practical security of PQC through cryptographic competitions.
  - By solving higher-dimensional cryptography, we can design optimal parameters that offer both security and efficiency.

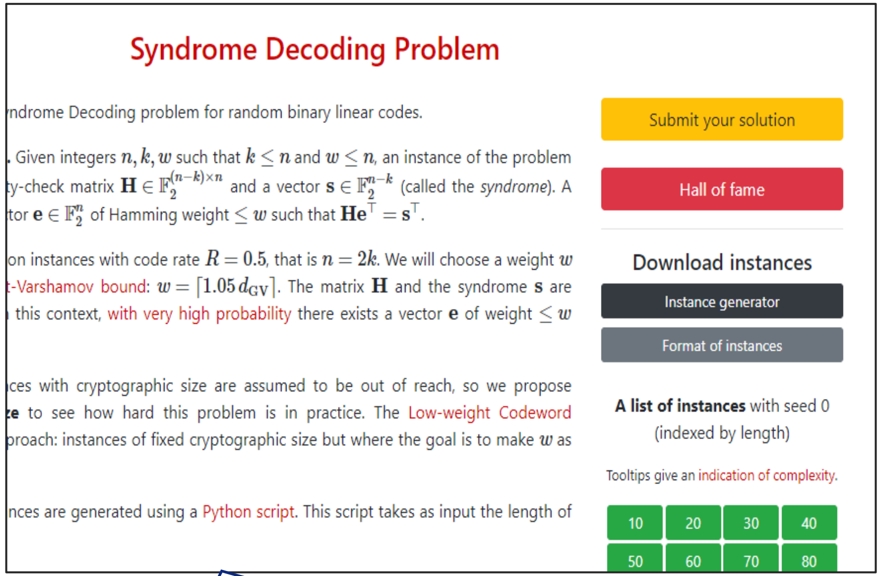
SVP Challenge
(Lattice-based Cryptography) 2013


SVP CHALLENGE

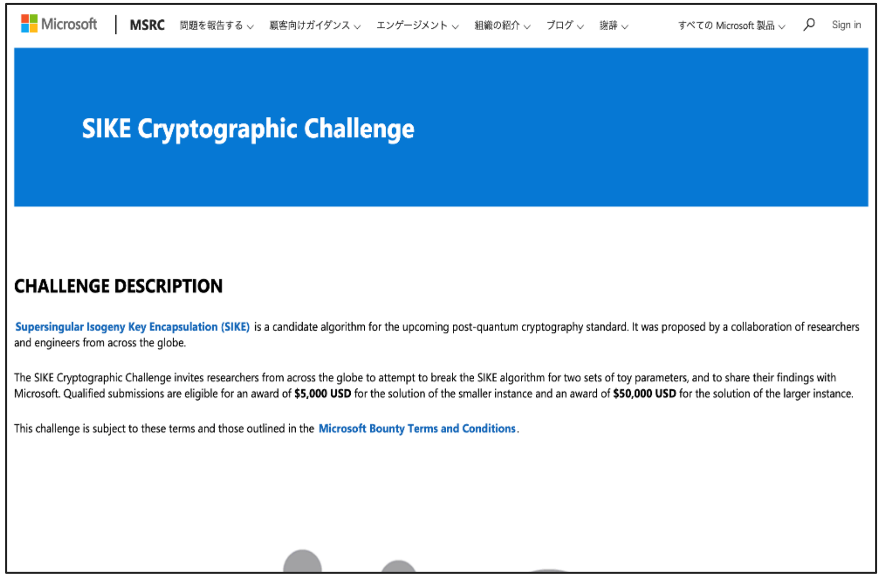
HALL OF FAME

Position	Dimension	Euclidean Norm	Seed	Contestant	Solution	Algorithm	Subm. Date	Approx. Factor
1	180	3509	0	L. Ducas, M. Stevens, W. van Woerden	vec	Sieving	2021-02-8	1.04002
2	178	3447	0	L. Ducas, M. Stevens, W. van Woerden	vec	Sieving	2021-02-8	1.02725
3	176	3487	0	L. Ducas, M. Stevens, W. van Woerden	vec	Sieving	2020-10-13	1.04411
4	170	3438	0	L. Ducas, M. Stevens, W. van Woerden	vec	Sieving	2020-05-12	1.04690
5	158	3240	0	Sho Hasegawa, Yuntao Wang, Eiichiro Fujisaki	vec	Sieving	2021-01-22	1.02311
6	157	3320	0	L. Ducas, M. Stevens, W. van Woerden	vec	Sieving	2019-05-20	1.04906
7	156	3219	0	Sho Hasegawa, Yuntao Wang, Eiichiro Fujisaki	vec	Sieving	2021-01-22	1.01986
8	155	3165	0	M. Albrecht, L. Ducas, G. Herold, E. Kirshanova, E. Postlethwaite, M.	vec	Sieving	2018-09-18	1.00803

Decoding Challenge
(Code-based Cryptography) 2019



SIKE Cryptographic Challenge
(Isogeny-Based Cryptography) 2021



It is hosted by Inria

Syndrome Decoding Problem (SDP)

Input: Positive integer n,k,w, matrix $\boldsymbol{H} \in \mathbb{F}_2^{(n-k)\times n}$ and $\boldsymbol{s} \in \mathbb{F}_2^{n-k}$
Output: A vector $\boldsymbol{e} \in \mathbb{F}_2^n$ that satisfies $\boldsymbol{He} = \boldsymbol{s}$ where $\mathrm{wt}(\boldsymbol{e}) = w$

$n = 8$
$k = 4$
$w = 3$

$\boldsymbol{H}$: Given

$\boldsymbol{s}$: Given

$\boldsymbol{h}_1$	$\boldsymbol{h}_2$	$\boldsymbol{h}_3$	$\boldsymbol{h}_4$	$\boldsymbol{h}_5$	$\boldsymbol{h}_6$	$\boldsymbol{h}_7$	$\boldsymbol{h}_8$
1	0	1	0	0	0	1	1
0	1	1	1	0	1	0	1
0	0	1	0	1	1	1	0
0	0	0	1	0	0	1	0

$\boldsymbol{s}$
1
1
1
1

$\boldsymbol{e} = 01110000$
(Solution)

Difficult to solve !
(If appropriate parameters are used)

Information Set Decoding (ISD)

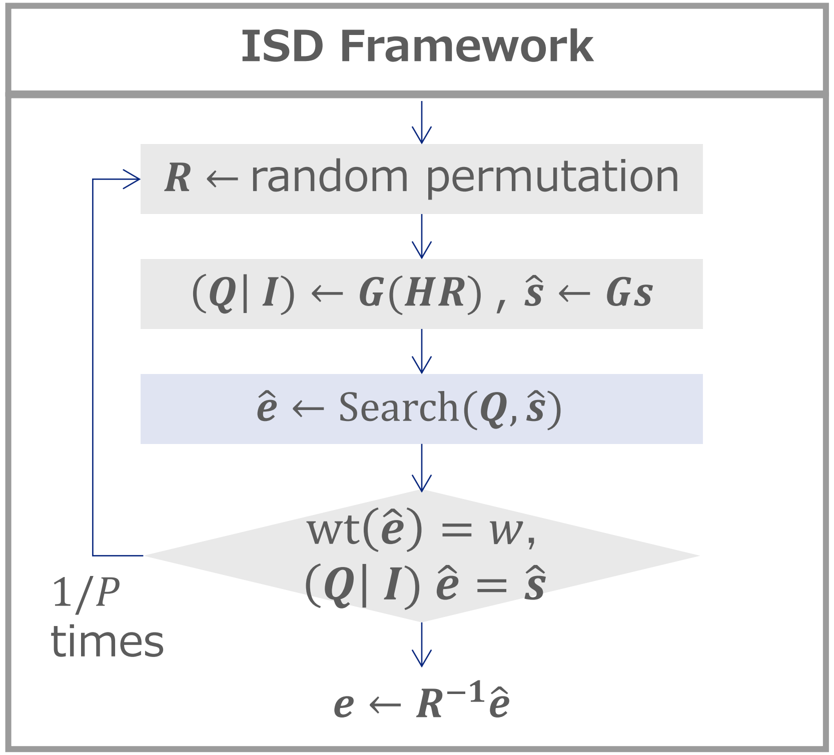
- Information Set Decoding (ISD) is used to solve SDP efficiently

Algorithm	Year	Asymptotic Time Complexity
Prange [1]	1962	$2^{0.121n}$
Dumer [2]	1991	$2^{0.117n}$
May-Meurer-Thomae (MMT)[3]	2011	$2^{0.112n}$
Becker-Joux-May-Meurer (BJMM)[4]	2012	$2^{0.102n}$
May-Ozerov (MO)[5]	2015	$2^{0.0953n}$
Both-May (BM) [6,7]	2018	$2^{0.0951n}$

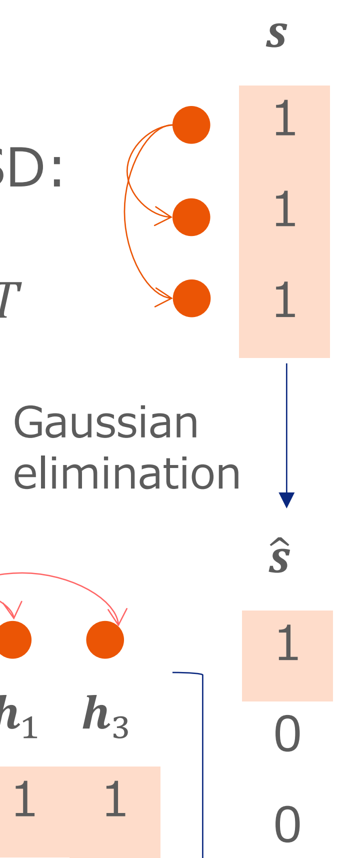
[1] E. Prange, "The use of information sets in decoding cyclic codes,"1962.
[2] I. Dumer, "On minimum distance decoding of linear codes,"1991.
[3] A. May, et al., "Decoding random linear codes in ˜O (20.054n) ," 2011.
[4] A. Becker, et al., "Decoding random binary linear codes in 2n/20: How 1 + 1 = 0 improves information set decoding," 2012
[5] A. May and I. Ozerov, "On computing nearest neighbors with applications to decoding of binary linear codes," 2015
[6] L. Both and A. May, "Decoding linear codes with high error rate and its impact for LPN security," 2018
[7] A. Esser, "Revisiting Nearest-Neighbor-Based Information Set Decoding", 2023

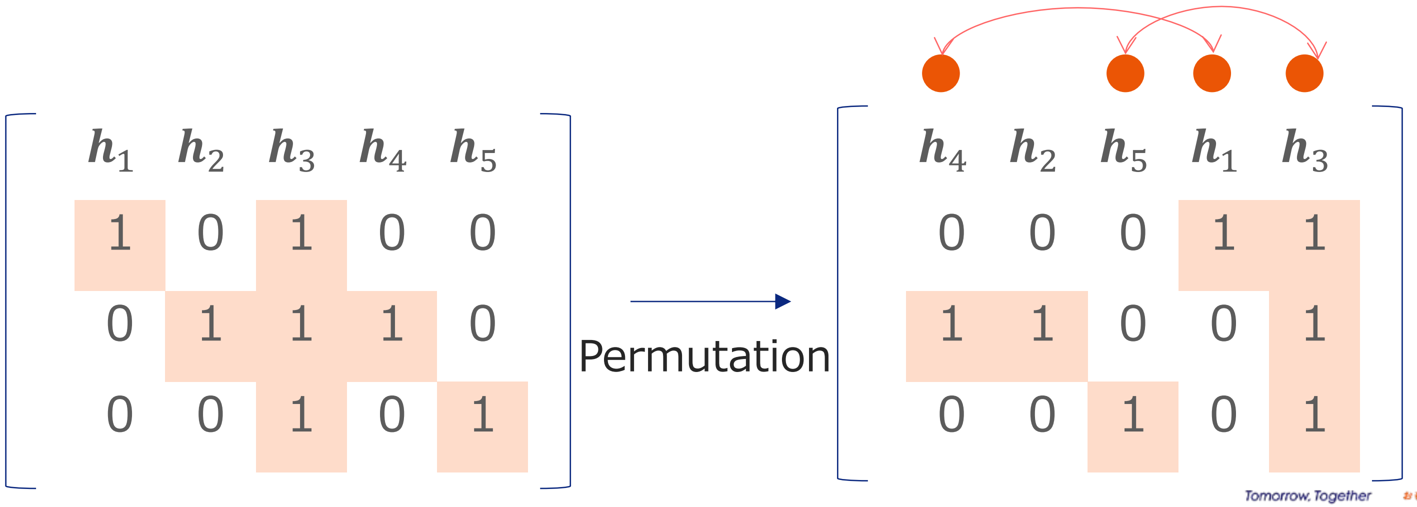
Common Framework of ISD

- ISD repeatedly executes permutation, Gaussian elimination, and solution search for an input matrix $\boldsymbol{H}$ and syndrome $\boldsymbol{s}$.



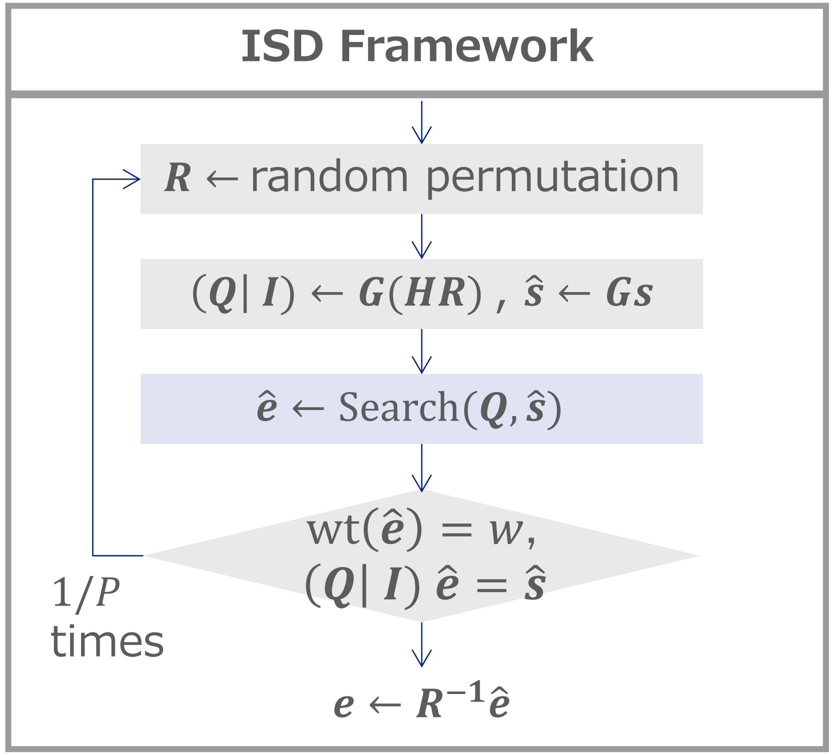
- Average time complexity (work factor) of ISD:
  - Decryption success prob. in one loop: P
  - Time complexity required for one loop: T
  - WF = T / P

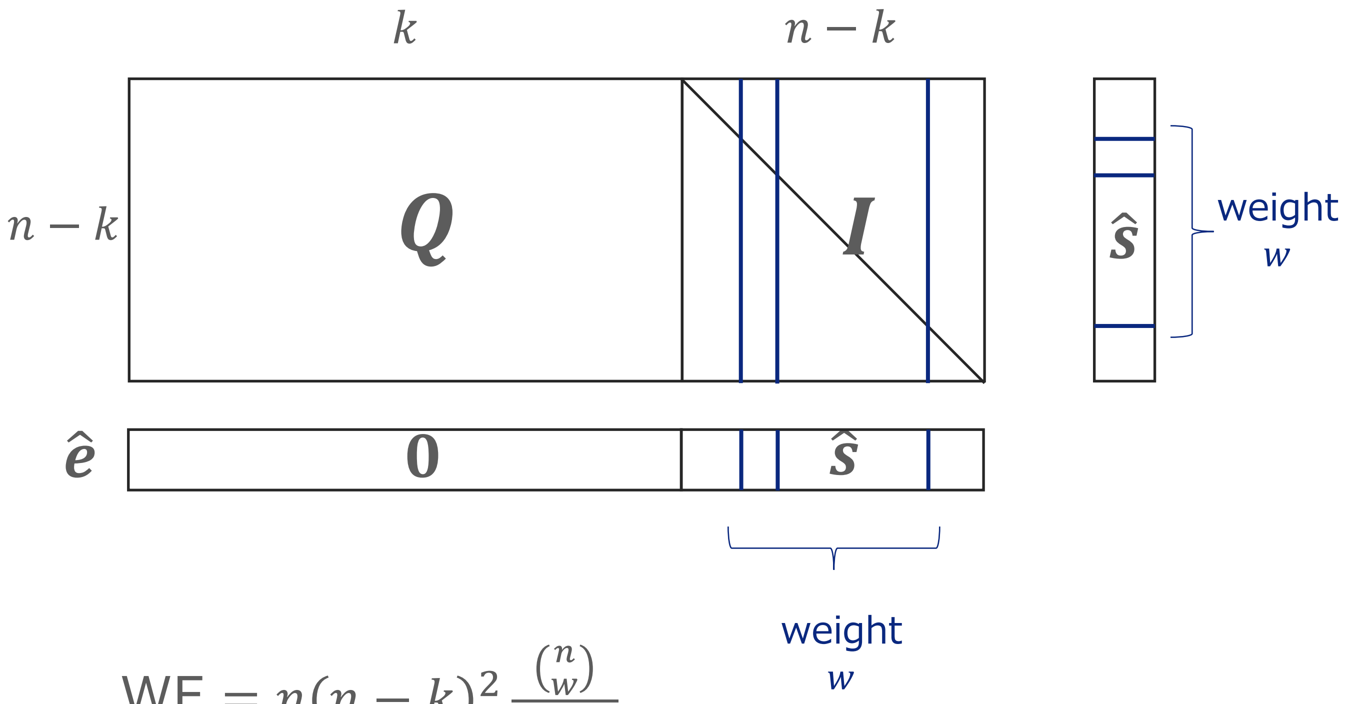




Prange's Algorithm

- Prange's algorithm is the world's first ISD algorithm.
  - It just checks the weight of $\hat{\boldsymbol{s}}$ in Search, if $\mathrm{wt}(\hat{\boldsymbol{s}}) = w$, the solution is $\boldsymbol{e} \leftarrow \boldsymbol{R}^{-1}(\boldsymbol{0}, \hat{\boldsymbol{s}})$.
  - It has a drastically smaller WF compared to naive search.

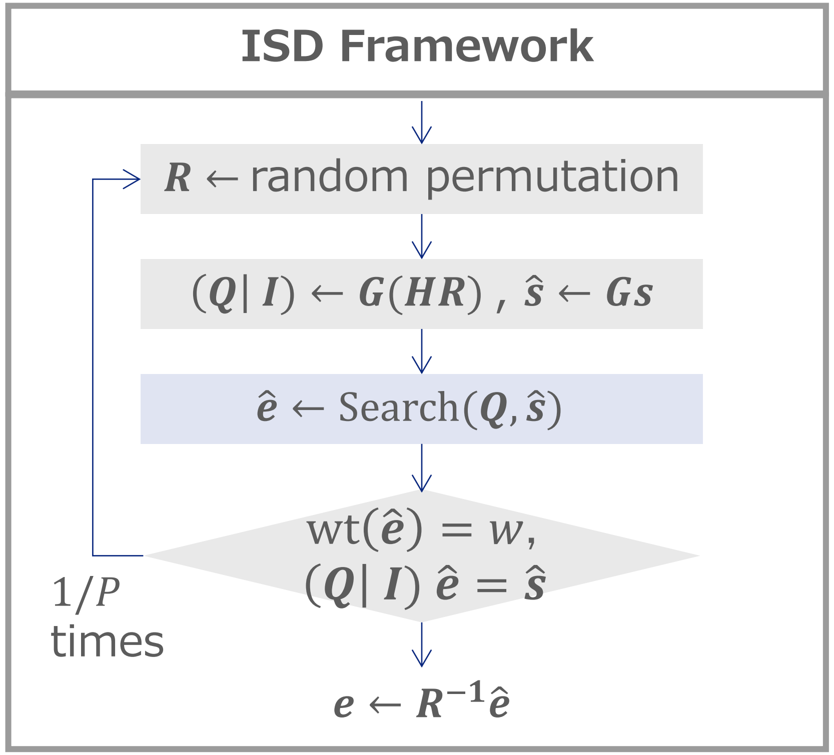


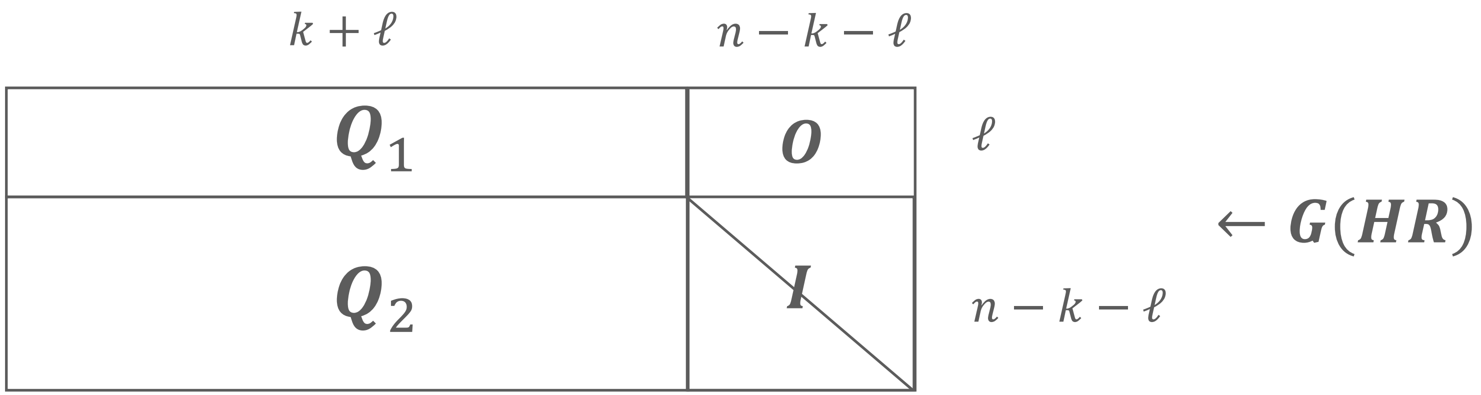


$$\mathrm{WF} = n(n-k)^2 \frac{\binom{n}{w}}{\binom{n-k}{w}}$$

Dumer's Algorithm

- Dumer's algorithm utilizes **2-lists merging** (birthday decode) to reduce the WF
- Success probability P significantly increases compared to Prange's ISD





- $P = \dfrac{\binom{(k+\ell)/2}{p}^2 \binom{n-k-\ell}{w-2p}}{\binom{n}{w}}$
- $T = n(n-k)^2 + |L_1| + \max\left(|L_1|, \dfrac{|L_1|^2}{2^\ell}\right)$
- WF $= T/P$

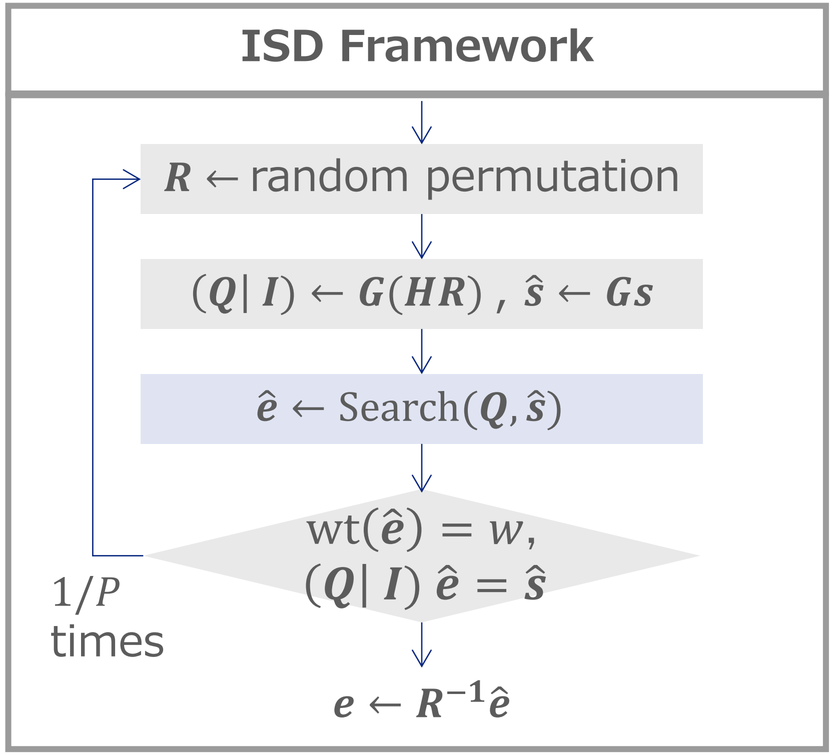
Prange's: $P = \dfrac{\binom{n-k}{w}}{\binom{n}{w}}$

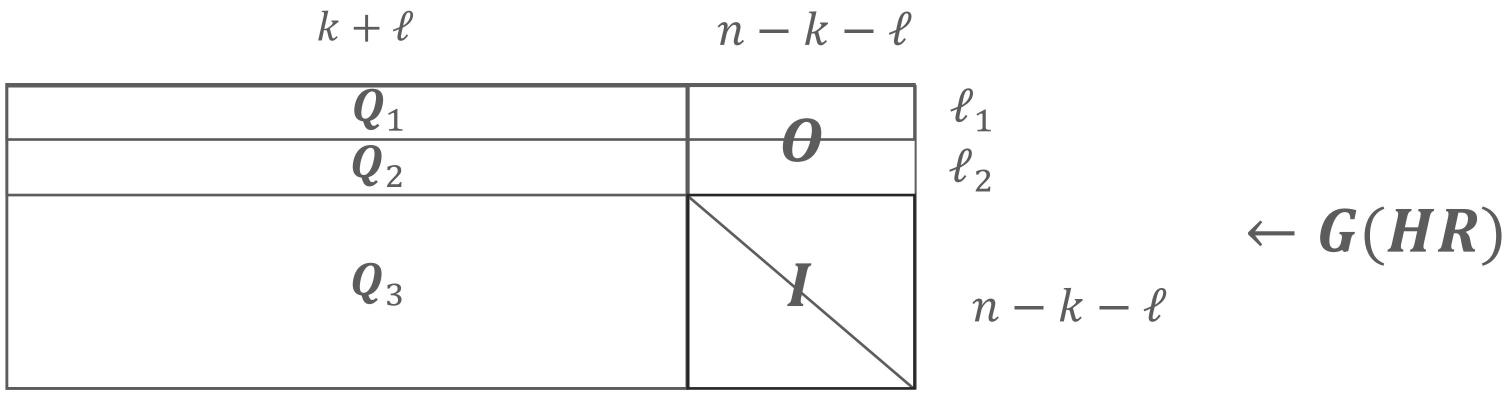
Prange's: $T = n(n-k)^2$

➔ For more details, Let's check web contents about ISD in **Canal-U TV** provided by Inria

May-Meurer-Thomae (MMT) Algorithm

- The MMT algorithm utilizes **4-lists merging** for a more efficient search
- A smaller T can be obtained for the same P as the Dumer's algorithm





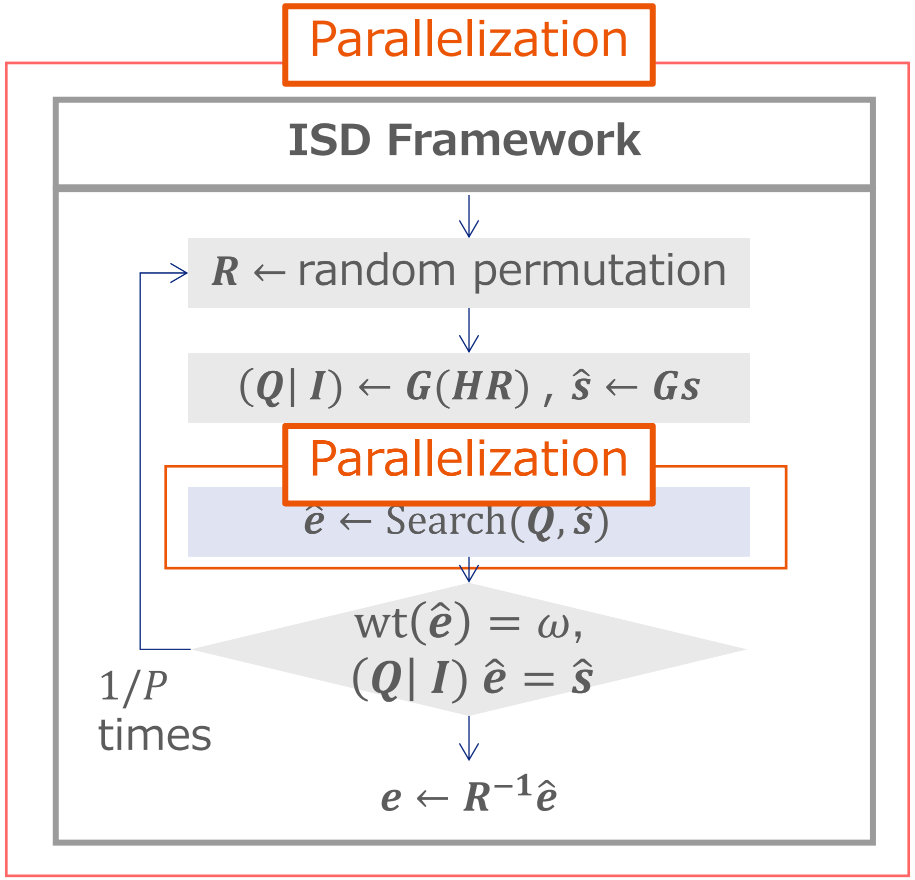
- $P = \dfrac{\binom{(k+\ell)/2}{p}^2 \binom{n-k-\ell}{w-2p}}{\binom{n}{w}}$
- $T = n(n-k)^2 + |L_{11}| + \max\left(|L_{11}|, \frac{|L_{11}|^2}{2^{\ell_1}}\right) + \max\left(|L_1|, \frac{|L_1|^2}{2^{\ell_2}}\right)$
- $\mathrm{WF} = T/P$

Dumer's:

$$T = n(n-k)^2 + |L_1| + \max\left(|L_1|, \frac{|L_1|^2}{2^{\ell}}\right)$$

Parallelized ISD Algorithms

- Significant acceleration through parallelization is indispensable for solving large-scale SDPs.
- We employ parallelization for the **entire** processes and for **internal** search.



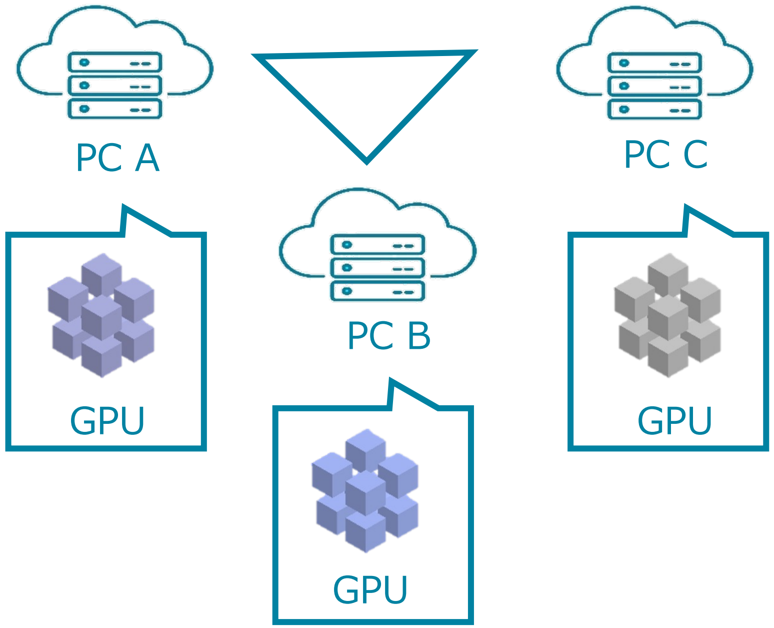
Paper	HW	Parallelization	ISD Algorithm
FPGA Stern Attack [1]	FPGA	Entire	Stern
Parallel MMT/BJMM [2]	CPU	Entire	MMT/BJMM
cuDumer [3]	GPU	Internal	Dumer
cuMMT [4]	GPU	Internal	MMT

[1] S. Heyse, et al. “Attacking code-based cryptosystems with information set decoding using special-purpose hardware,” 2014
[2] A. Esser, et al. “McEliece needs a break – solving McEliece-1284 and Quasi-Cyclic-2918 with modern ISD,” 2022
[3] S. Narisada, et al. “Fast GPU implementation of dumer’s algorithm solving the syndrome decoding problem,” 2021.
[4] S. Narisada, et al. “Multiparallel MMT : Faster ISD Algorithm Solving High-Dimensional Syndrome Decoding Problem,” 2022.

Hardware Configuration

- We use several PC/Servers to solve large-scale SDP
- Local PC i) :Desktop PC equipped with a dedicated GPGPU board: **NVIDIA Tesla V100S**.
- Local PC ii): Desktop PC equipped with a general-purpose GPU board: **GeForce RTX 4080**.
- Cloud Server: AWS P3 instance (p3.2xlarge, with a **NVIDIA Tesla V100**)

Local PC i) in our lab
(with a circulator fan for cooling)



Experimental Results of cuMMT

- Decryption results in the Decoding Challenge:

SDP instance (n, k, ω)	Difficulty to solve	HW Configuration	# of PC/Servers	Actual decryption time
SDP(510,255,62)	2^{54}	Local PC (i)	4	24.7 days
SDP(530,260,65)	2^{56}	Local PC (i)	4	12.5 days
SDP(540,270,66)	2^{57}	Cloud Server	22	79.4 days
SDP(550,275,67)	2^{58}	Local PC (i)	4	13.0 days
SDP(570,285,70)	2^{60}	Local PC (ii)	10	45.3 days
SDP(1409,1127,26)	2^{63}	Local PC (ii)	10	30 hours (70 days expected)

Memory usage of cuMMT per one Local PC (ii) : **800 [MB]**

Results of Decoding Challenge (as of Dec. 29, 2023)

SDP Challenge

Home | Generic problems | NIST-like problems | Documentation | Contact

Syndrome Decoding Problem

Hall of Fame

WF: 2^{60}

Length	Weight	Authors	Algorithm	Date	Details
570	70	Shintaro Narisada, Kazuhide Fukushima, and Shinsaku Kiyomoto	MMT variant	2023-04-17	See details
550	67	Shintaro Narisada, Kazuhide Fukushima, and Shinsaku Kiyomoto	MMT	2022-02-23	See details
540	66	Shintaro Narisada, Kazuhide Fukushima, and Shinsaku Kiyomoto	MMT	2022-02-01	See details
530	65	Shintaro Narisada, Kazuhide Fukushima, and Shinsaku Kiyomoto	MMT	2021-10-27	See details
510	61	Shintaro Narisada, Kazuhide Fukushima, and Shinsaku Kiyomoto	MMT	2021-09-19	See details
500	59	Greg Meyer	Dumer	2020-07-27	See details
490	59	Greg Meyer	Dumer	2020-08-	See

Results of Decoding Challenge (as of Dec. 29, 2023)

Goppa McEliece Challenge

Home Generic problems NIST-like problems Documentation Contact

Syndrome Decoding in the Goppa-McEliece Setting

Hall of Fame

WF : 2^{63}

Length	Weight	Authors	Algorithm	Date	Details
1409	26	Shintaro Narisada, Hiroki Furue, Yusuke Aikawa, Kazuhide Fukushima, and Shinsaku Kiyomoto	MMT variant	2023-11-13	See details
1347	25	Daniel J. Bernstein, Tanja Lange, Christiane Peters	See https://isd.mceliece.org/1347.html for more information.	2023-02-24	See details
1284	24	Andre Esser, Alex May and Floyd Zweydinger	MMT variant	2021-08-16	See details
1223	23	Andre Esser, Alex May and Floyd Zweydinger	BJMM/MMT variant	2021-05-10	See details
1161	22	Shintaro Narisada, Kazuhide Fukushima, and Shinsaku Kiyomoto	Dumer	2021-01-10	See details
1101	21	Anders Nilson	Multi threads Dumer4, Gregory Landais impl.	2020-08-14	See details

Ultra High-Speed Symmetric Cryptography: Rocca-S

Use Cases for 6G: Need for Ultra High-Speed Encryption

Communication exceeding 100Gbps is expected in various use cases.*

Immersive Experiences
Enabled by Advanced XR Technologies

XR (Extended Reality) with Multiple Sensors

High-Definition **Holograms**

Data Collection from Massive Sensors

(*) KEY DRIVERS AND RESEARCH CHALLENGES FOR 6G UBIQUITOUS WIRELESS INTELLIGENCE http://jultika.oulu.fi/files/isbn9789526223544.pdf

Overview of Rocca-S

The world's first symmetric cryptography that meets all the requirements of 6G.

- Rocca-S achieves speeds exceeding **200Gbps** (SW) and **2Tbps** (HW), establishing itself as the world's fastest stream cipher for the 6G era.
- It supports **256-bit keys** and incorporates both data encryption and **data authentication** features.

Origin of the name Rocca-S

- We have selected the term "**Rocca**" as a uniquely Japanese word from among the candidates with a sound similar to “**Roku**" (six in Japanese) in the context of 6G.
- "**Rocca**" means **fortress** in Italian and reflects our intention to design robust cryptography.

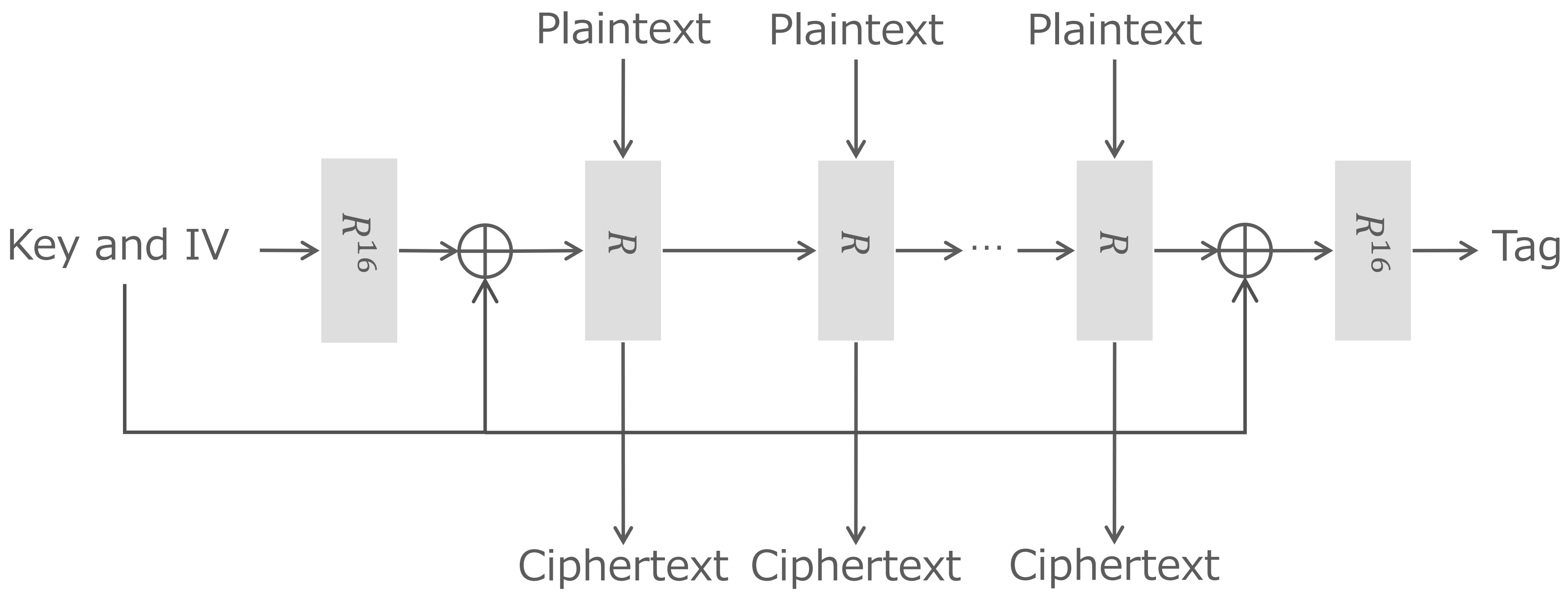
Performance Results

Rocca-S achieves performance exceeding 200Gbps on PCs and over 90Gbps on smartphones.

Devices	Model name/ CPU	Performance [Gbps]
PC	Intel® Core i7™ (13th Generation)	234 Gbps (Encryption only) 207 Gbps (Authenticated encryption)
	Intel® Core i9™(13th Generation)	254 Gbps (Encryption only) 227 Gbps (Authenticated encryption)
Smartphone	iPhone 14 Pro Max / Apple A16 Bionic	93.0 Gbps (Encryption only) 87.4 Gbps (Authenticated encryption)
	Galaxy Z Flip4 / Snapdragon 8+ Gen 1	71.5 Gbps (Encryption only) 66.2 Gbps (Authenticated encryption)
	iPhone 13 / Apple A15 Bionic	86.2 Gbps (Encryption only) 76.4 Gbps (Authenticated encryption)
	Google Pixel 3 / Snapdragon 845	33.9 Gbps (Encryption only) 31.1 Gbps (Authenticated encryption)

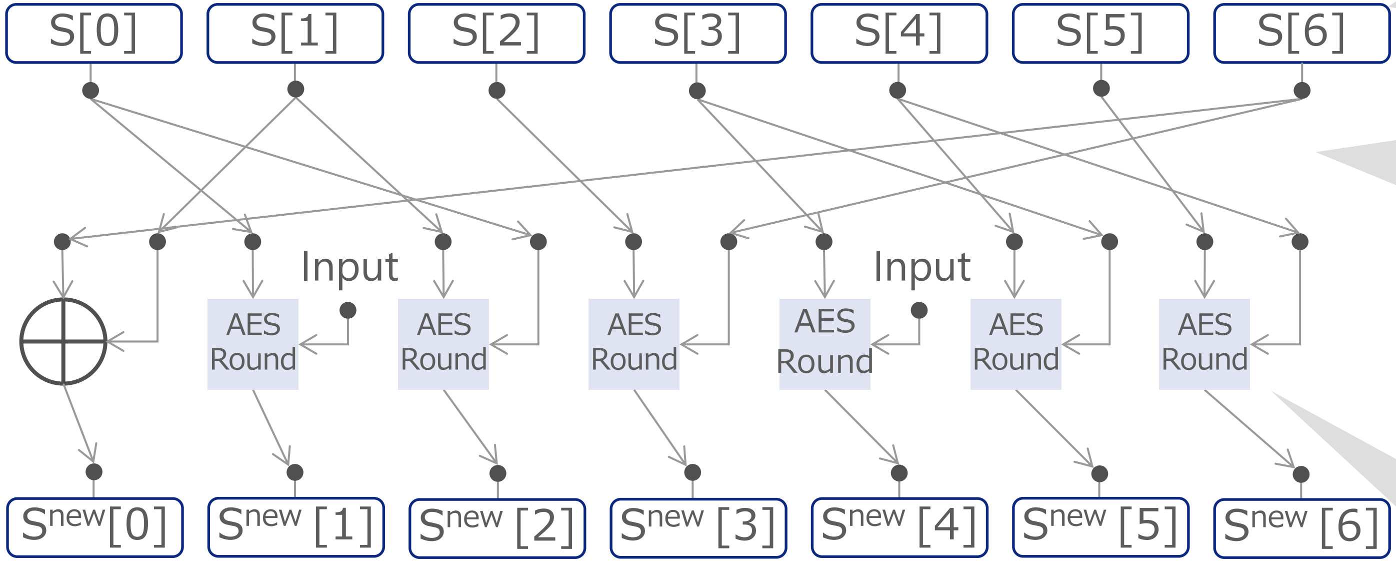
Features of Rocca-S (1/2)

Rocca-S incorporates both data encryption and data authentication features.



Features of Rocca-S (2/2)

Rocca-S maximizes encryption processing speed to the utmost limits.



Optimal parallelization

Rocca-S processes **multiple blocks in parallel** and make the amount of arithmetic processing for each block uniform to achieve better performance.

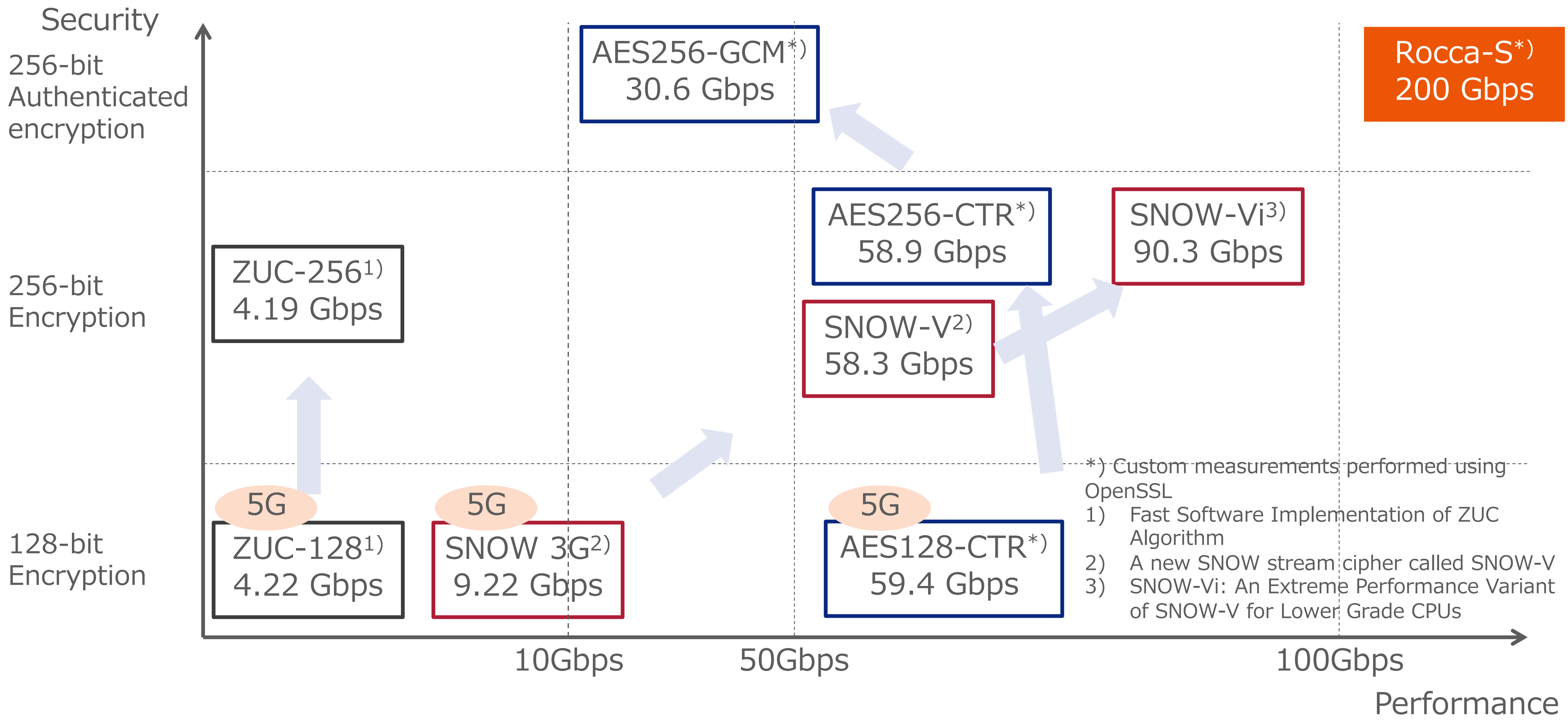
Optimal block-to-block connection structure

Rocca-S selects the connection structure that achieve the **best balance of security and performance** from 13 million candidates.

Utilization of hardware instructions

Rocca-S achieves acceleration by employing the AES round function and utilizing CPU hardware instructions (such as **AES-NI**).

Comparison with Symmetric Cryptography in 5G (on Intel Core i7)



*) Custom measurements performed using OpenSSL

1) Fast Software Implementation of ZUC Algorithm
2) A new SNOW stream cipher called SNOW-V
3) SNOW-Vi: An Extreme Performance Variant of SNOW-V for Lower Grade CPUs

Thank you!

McEliece Cryptosystem

- Encryption: $\boldsymbol{c} = \boldsymbol{m}\widehat{\boldsymbol{G}} + \boldsymbol{e}$ $\quad (\boldsymbol{y}, \boldsymbol{e} \in \mathbb{F}_2^n, \boldsymbol{x} \in \mathbb{F}_2^k, \widehat{\boldsymbol{G}} \in \mathbb{F}_2^{k\times n}$ where $\mathrm{wt}(\boldsymbol{e}) = w$, $\widehat{\boldsymbol{G}} = \boldsymbol{SGP})$

  Ciphertext ($\boldsymbol{c}$), Plaintext ($\boldsymbol{m}$), Public key ($\widehat{\boldsymbol{G}}$), Noise ($\boldsymbol{e}$), Secret key ($\boldsymbol{SGP}$)

- Decryption: $\boldsymbol{cP}^{-1} = \boldsymbol{mSG} + \boldsymbol{eP}^{-1}$ ➔ $\mathrm{decode}(\boldsymbol{mSG} + \boldsymbol{eP}^{-1}) = \boldsymbol{mS}$ ➔ $(\boldsymbol{mS})\boldsymbol{S}^{-1} = \boldsymbol{m}$

  Ciphertext ($\boldsymbol{c}$), Secret key ($\boldsymbol{P}^{-1}$), Secret key ($\boldsymbol{S}^{-1}$)

- Example:
  - Encryption : $\begin{bmatrix} 1 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix}$

    Ciphertext = Plaintext × Public key + Noise

Message Attack : An attacker try to restore secret information ($\boldsymbol{m}$ or $\boldsymbol{e}$) from public information ($\boldsymbol{c}$ and $\widehat{\boldsymbol{G}}$).

Requirements for Symmetric Cryptography in the 6G Era

New symmetric cryptography is expected to meet the anticipated requirements for 2030 and beyond.

Support for High-Speed and High-Capacity Communication

- Symmetric cryptography shall achieve **processing speeds of 100Gbps or higher** without causing any bottlenecks to ensure compatibility with the fast and high-capacity utilization in 6G.

Resistance to Quantum Computers

- Symmetric cryptography shall support a **key length of 256 bits**, which is twice as the current requirement for (4G/5G) to protect against large-scale quantum computers.

Compliance with Security Requirements Adopted in IETF

- Multiple vulnerabilities have occurred in the past due to improper use of encryption, such as OpenSSL. Symmetric cryptography shall **have data authentication feature (authentication encryption)** to address this issue at its core.