Mitigation on AIM Cryptanalysis

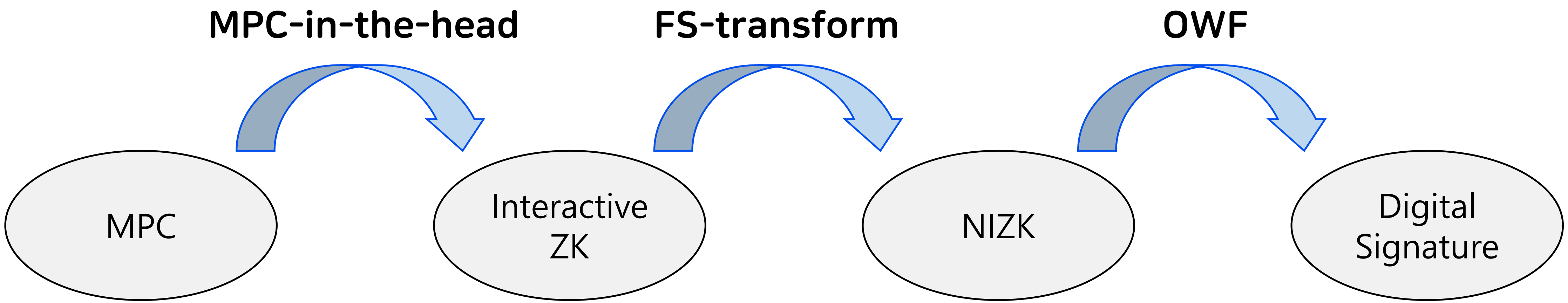
Seongkwang Kim[1] Jihoon Cho[1]
Mingyu Cho[1] **Jincheol Ha[2]**
Jihoon Kwon[1] Byeonghak Lee[1]
Joohee Lee[3] Jooyoung Lee[2]
Sangyub Lee[1] Dukjae Moon[1]
Mincheol Son[2] Hyojin Yoon[1]

[1] Samsung SDS, Seoul, Korea
[2] KAIST, Daejeon, Korea
[3] Sungshin Women's University, Seoul, Korea

KpqC 7th Workshop

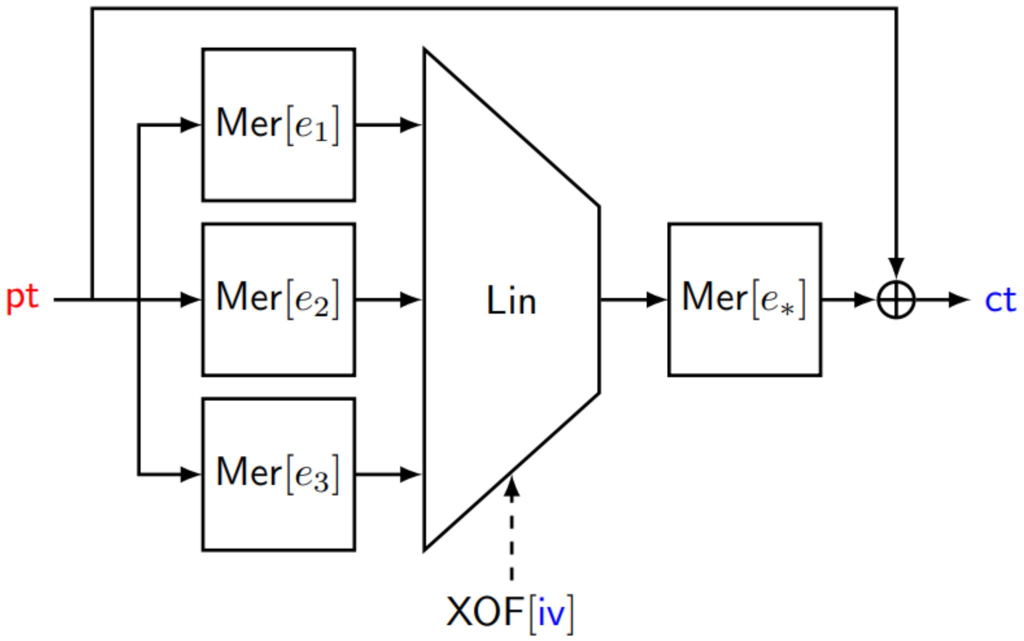
Recap on AIM and AIMer

MPCitH-based Digital Signature



- MPCitH protocol + One-way function ⇒ Digital signature
- BN++ protocol + AIM ⇒ AIMer signature

Symmetric Primitive AIM



Scheme	λ	n	ℓ	e_1	e_2	e_3	e_*
AIM-I	128	128	2	3	27	-	5
AIM-III	192	192	2	5	29	-	7
AIM-V	256	256	3	3	53	7	5

- Mersenne S-box
  - Invertible, high-degree, quadratic relation
  - Requires a single multiplication
  - Produces $3n$ quadratic equations
  - Moderate DC/LC resistance
- Repetitive structure
  - Parallel application of S-boxes
  - Feed-forward construction
  - Fully exploit the BN++ optimizations
  - Locally-computable output share
- Randomized structure
  - Affine layer is generated from XOF

AIMer Signature Scheme

- AIMer = BN++ proof of knowledge of AIM input
- Security is based on the one-wayness of AIM in the ROM
- Advantages
  - Security based on only symmetric primitives
  - Fast key generation
  - Small key sizes
  - Trade-offs between signatures size and speed
  - Randomness misuse resistance
- Limitations
  - Newly-designed symmetric primitive AIM
  - Moderately large signature size (3.8~5.9 KB)
  - Slow signing/verifying speed (0.59~22 ms)

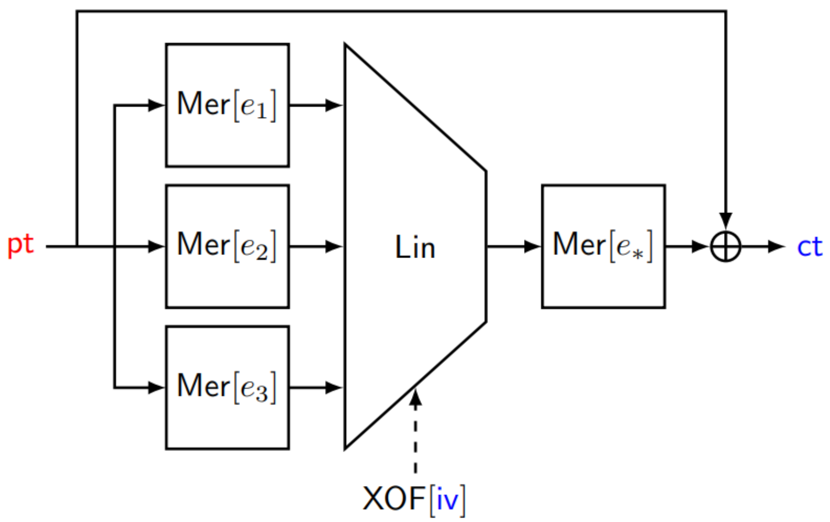
Scheme	pk (B)	sig (B)	Sign (ms)	Verify (ms)
Dilithium2	1312	2420	0.10	0.03
Falcon-512	897	690	0.27	0.04
SPHINCS$^+$-128s	32	7856	315.74	0.35
SPHINCS$^+$-128f	32	17088	16.32	0.97
Picnic1-L1-full	32	30925	1.16	0.91
Picnic3	32	12463	5.83	4.24
Banquet	32	19776	7.09	5.24
Rainier$_3$	32	8544	0.97	0.89
BN++Rain$_3$	32	6432	0.83	0.77
AIMer-L1	32	5904	0.59	0.53
AIMer-L1	32	3840	22.29	21.09

Analyses on AIM

Recent Analysis on AIM

- Recent algebraic analysis on the symmetric primitive AIM
  - Fukang Liu, et al. "Algebraic Attacks on RAIN and AIM Using Equivalent Representations". Cryptology ePrint Archive. Report 2023/1133
  - Private communication with Fukang Liu
  - Markku-Juhani O. Saarinen. "Round 1 (Additional Signatures) OFFICIAL COMMENT: AIMER", pqc-forum. https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/BI2ilXblNy0
  - Kaiyi Zhang, et al. "Algebraic Attacks on Round-Reduced RAIN and Full AIM-III". ASIACRYPT 2023.
- There are two vulnerabilities in the structure of AIM
  - Low degree equations in n variables ⇒ Fast algebraic attack (w/ memory optimization)
  - Common input to the parallel Mersenne S-boxes ⇒ Structural vulnerability

Fast Algebraic Attack

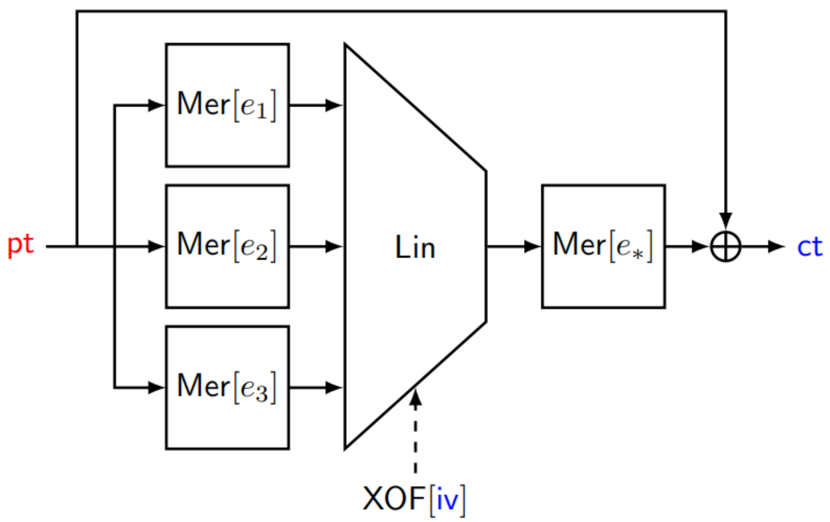


- Build low degree equations in n Boolean variables and apply the fast exhaustive search attack with memory-efficient Möbius transform.

	n	Degree	Time [bits]	Memory [bits]
AIM-I	128	10	$2^{136.2}$ (-10.2)	$2^{61.7}$
AIM-III	192	14	$2^{200.7}$ (-11.2)	$2^{84.3}$
AIM-V	256	15	$2^{265.0}$ (-12.0)	$2^{95.1}$

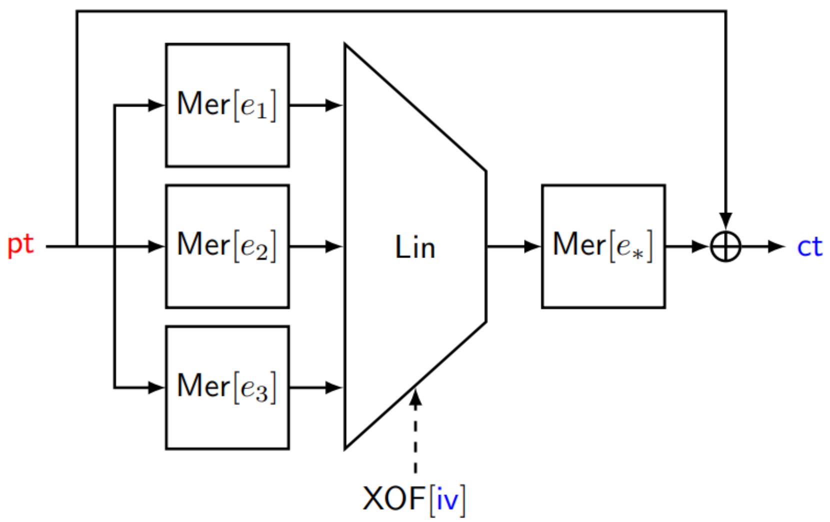
* Compared to the claimed security level

Structural Vulnerability



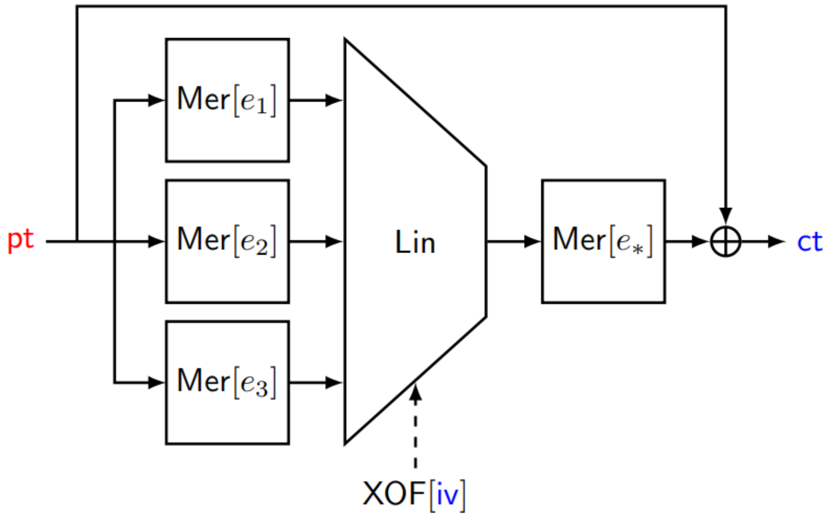
- Let $w = \mathrm{pt}^{-1}$ then $\mathrm{Mer}[e](\mathrm{pt}) \coloneqq \mathrm{pt}^{2^e-1} = \mathrm{pt}^{2^e} w$.
- A $2n$-variable system having
  - $5n$ quadratic equations (from $w = \mathrm{pt}^{-1}$) and
  - $5n$ cubic equations (from $\mathrm{Mer}[e_*]$)
- No practical attack exists on the above system, but the system is not considered in the first proposal.

Structural Vulnerability



- Let $w = \mathrm{pt}^{-1}$ then $\mathrm{Mer}[e](\mathrm{pt}) \coloneqq \mathrm{pt}^{2^e - 1} = \mathrm{pt}^{2^e} w$.
- $\mathrm{Mer}[e_i](\mathrm{pt}) = \mathrm{pt}^{2^{e_i}} \cdot w$ for $i = 1, \dots, \ell$ can be computed by precomputing the linear matrices for $E_i\colon \mathrm{pt} \mapsto \mathrm{pt}^{2^{e_i}}$.
- (e.g.) AIM-I
  - $\mathrm{ct} = \left(\mathrm{pt}^{2^3 - 1} \cdot A_1 + \mathrm{pt}^{2^{27} - 1} \cdot A_2 + b\right)^{2^5 - 1} + \mathrm{pt}$
  - $\begin{cases} u = \mathrm{pt} \cdot E_3 \cdot w \cdot A_1 + \mathrm{pt} \cdot E_{27} \cdot w \cdot A_2 + b \\ u \cdot E_5 = (\mathrm{ct} + \mathrm{pt}) \cdot u \end{cases}$

Structural Vulnerability

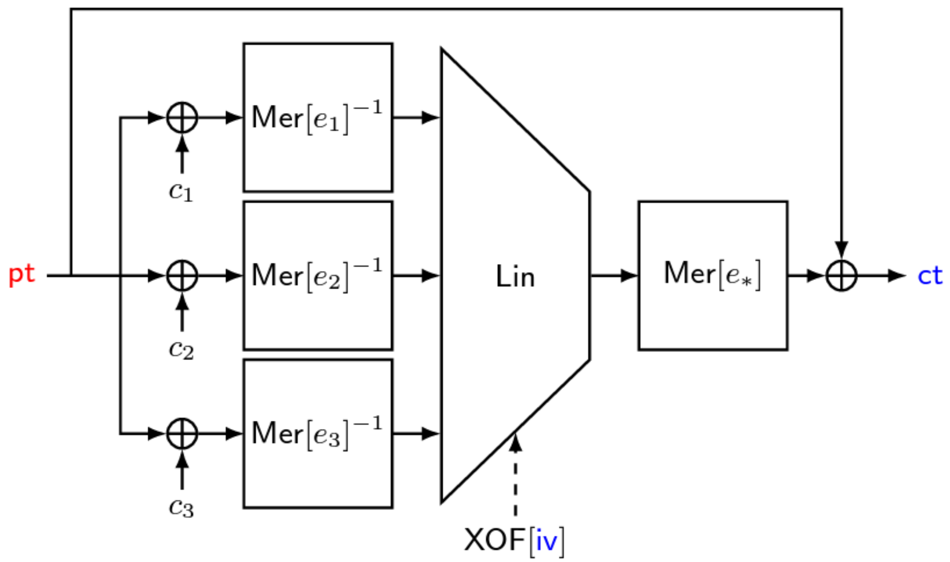


- Let $\mathrm{Mer}[e_i](\mathrm{pt}) = \left(\mathrm{pt}^d\right)^{s_i} \cdot \mathrm{pt}^{2^{t_i}}$ for some $d \mid 2^n - 1$ and guess the value of pt^d.
- The Mersenne S-boxes are linearized by the guessing.

	n	d	Time [enc]
AIM-I	128	5	$2^{125.7}$ (-2.3)
AIM-III	192	45	$2^{186.5}$ (-5.5)
AIM-V	256	3	$2^{254.4}$ (-1.6)

* Compared to the claimed security level

AIM2: Secure Patch for Algebraic Attacks



Scheme	λ	n	ℓ	e_1	e_2	e_3	e_*
AIM2-I	128	128	2	49	91	-	3
AIM2-III	192	192	2	17	47	-	5
AIM2-V	256	256	3	11	141	7	3

- Inverse Mersenne S-box
  - $\mathrm{Mer}[e]^{-1}(x) = x^a$
  - $a = (2^e - 1)^{-1} \bmod (2^n - 1)$
  - More resistant to algebraic attacks
- Larger exponents
  - To mitigate fast exhaustive search
- Fixed constant addition
  - To differentiate inputs of S-boxes
  - Increase the degree of composite power function

$$(x^a)^b \text{ vs } (x^a + c)^b$$

* S. Kim, et al. "Mitigation on the AIM Cryptanalysis". Cryptology ePrint Archive. Report 2023/1474

Analysis on AIM2

- Algebraic attacks
  - Fast exhaustive search: mitigated by high exponents
  - Brute-force search of quadratic equations
  - Toy experiment of good intermediate variables
- Other attacks
  - Exhaustive key search: slightly increased complexity
  - LC/DC: almost same
  - Quantum attacks: complexities change not critically
- Performance
  - Signature size: exactly the same
  - Sign/verify time: about 10% increase

Thank you!
Check out our website!