

AIM에 대한 분석 및 대응

Seongkwang Kim¹

Mingyu Cho¹

Jihoon Kwon¹

Joohee Lee³

Sangyub Lee¹

Mincheol Son²

Jihoon Cho¹

Jincheol Ha²

Byeonghak Lee¹

Jooyoung Lee²

Dukjae Moon¹

Hyojin Yoon¹

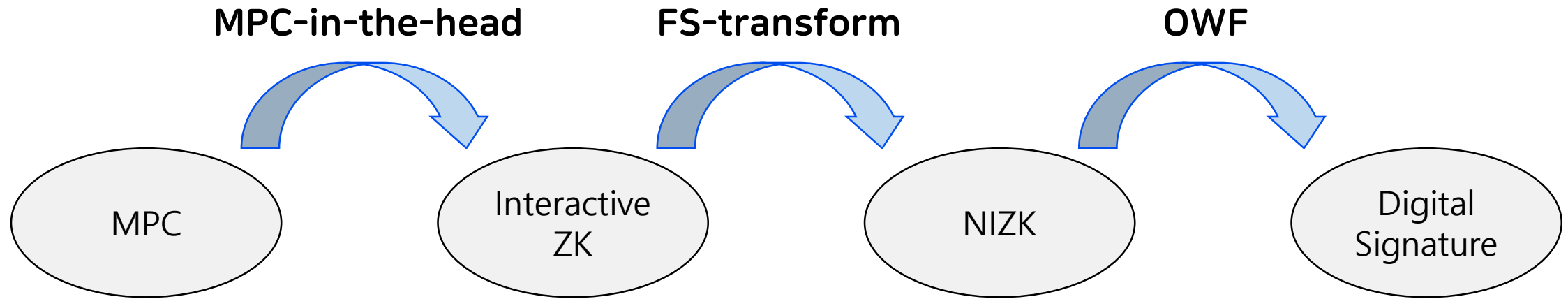
¹ Samsung SDS, Seoul, Korea

² KAIST, Daejeon, Korea

³ Sungshin Women's University, Seoul, Korea

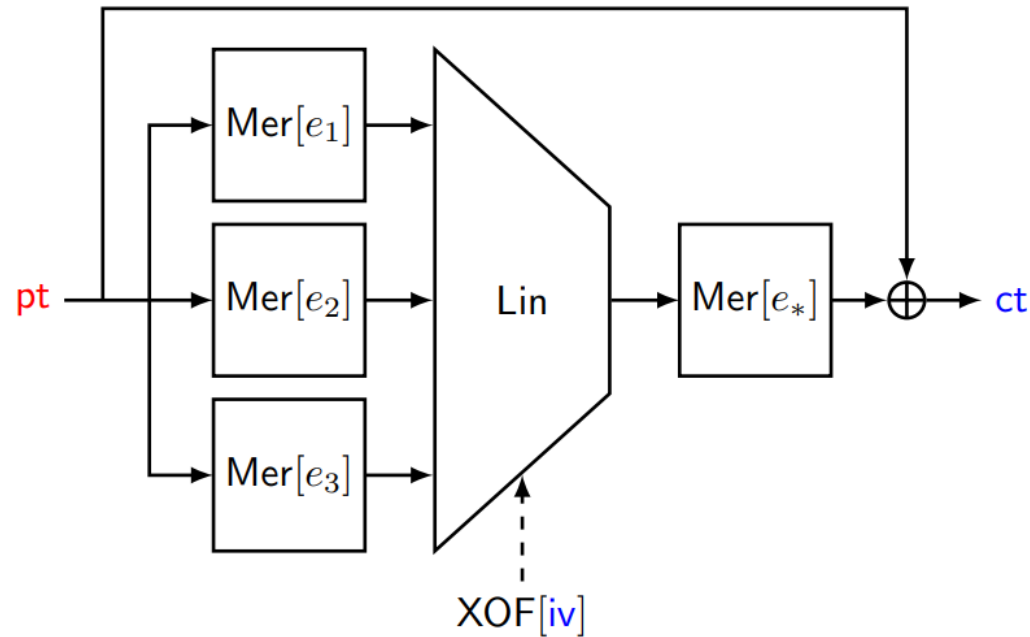
Recap on AIM and AIMer

MPCitH-based Digital Signature



- MPCitH protocol + One-way function \Rightarrow Digital signature
- BN++ protocol + AIM \Rightarrow AlMer 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

AlMer Signature Scheme

- AlMer = 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)

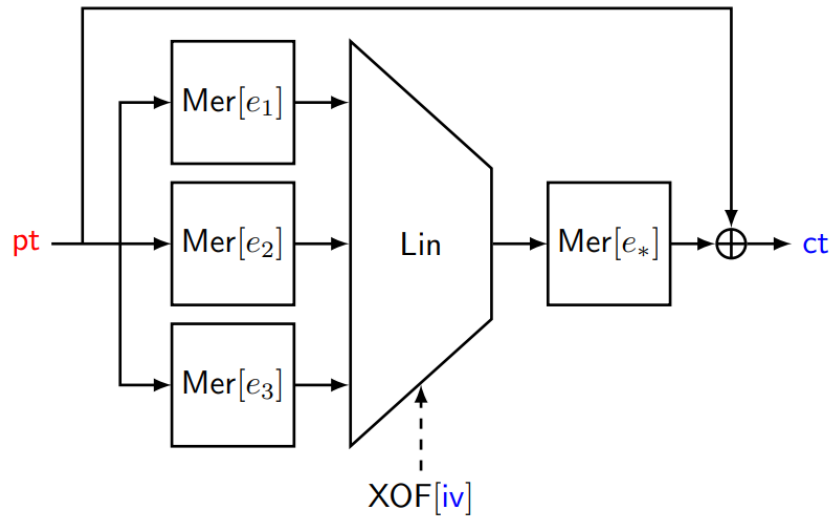
Scheme	pk (B)	sig (B)	Sign (ms)	Verify (ms)
Dilithium2	1312	2420	0.10	0.03
Falcon-512	897	690	0.27	0.04
SPHINCS+-128s	32	7856	315.74	0.35
SPHINCS+-128f	32	17088	16.32	0.97
Picnic1-L1-full	32	30925	1.16	0.91
Picnic3	32	12463	5.83	4.24
Banquet	32	19776	7.09	5.24
Rainier ₃	32	8544	0.97	0.89
BN++Rain ₃	32	6432	0.83	0.77
AlMer-L1	32	5904	0.59	0.53
AlMer-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 \Rightarrow Fast algebraic attack (w/ memory optimization)
 - Common input to the parallel Mersenne S-boxes \Rightarrow Structural vulnerability

Fast Algebraic Attack

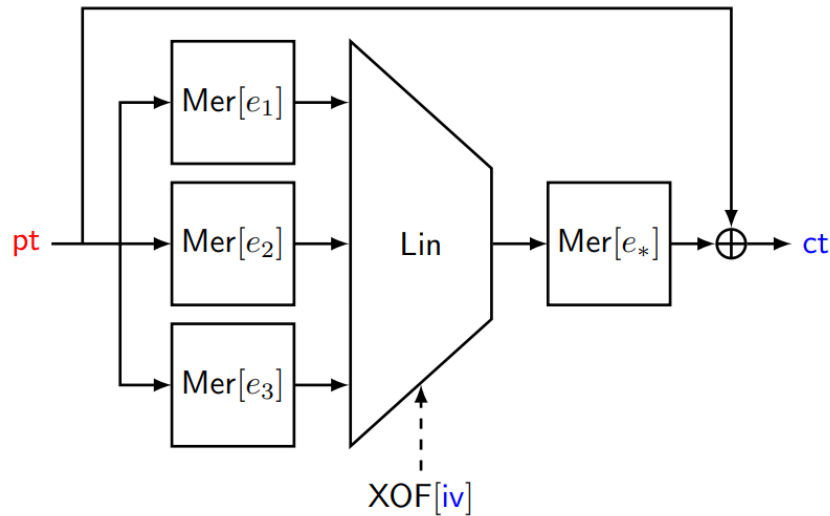


- Build low degree equations in n Boolean variables and apply the fast exhaustive search attack with memory-efficient Möbius transform.

	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)	$2^{95.1}$

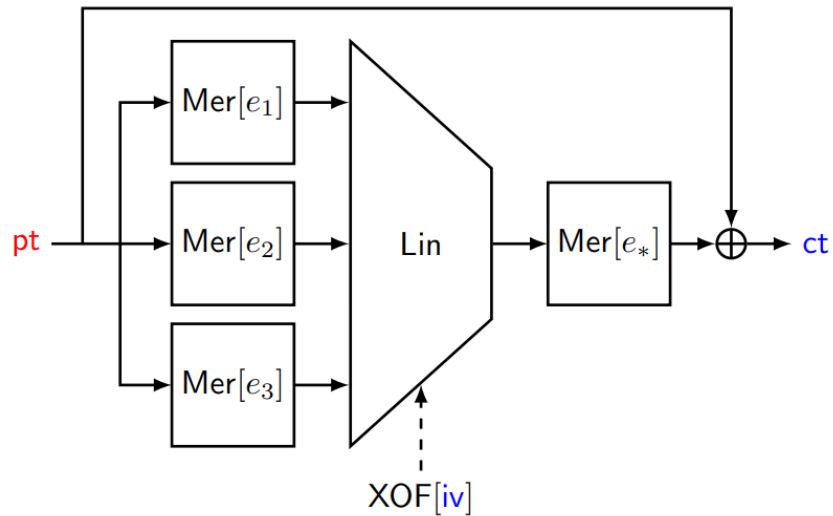
* Compared to the claimed security level

Structural Vulnerability



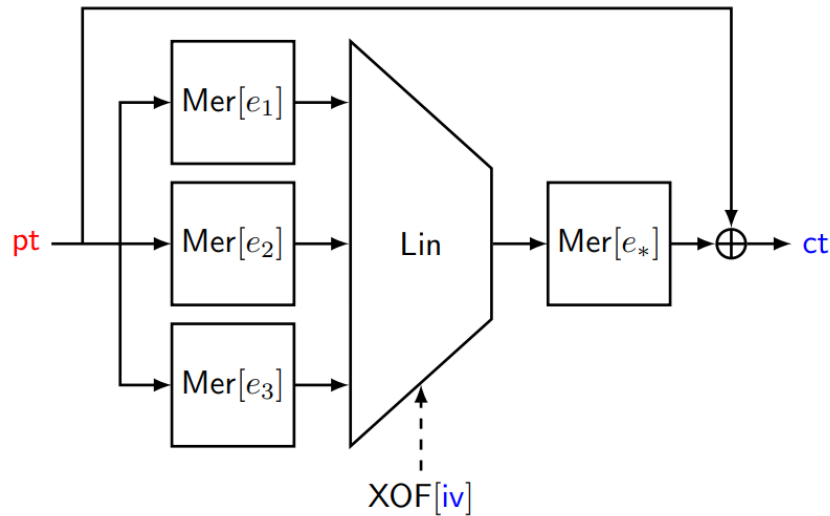
- Let $w = pt^{-1}$ then $Mer[e](pt) := pt^{2^e-1} = pt^{2^e} w$.
- A $2n$ -variable system having
 - $5n$ quadratic equations (from $w = pt^{-1}$) and
 - $5n$ cubic equations (from $Mer[e_*]$)
- No practical attack exists on the above system, but the system is not considered in the first proposal.

Structural Vulnerability



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

Structural Vulnerability

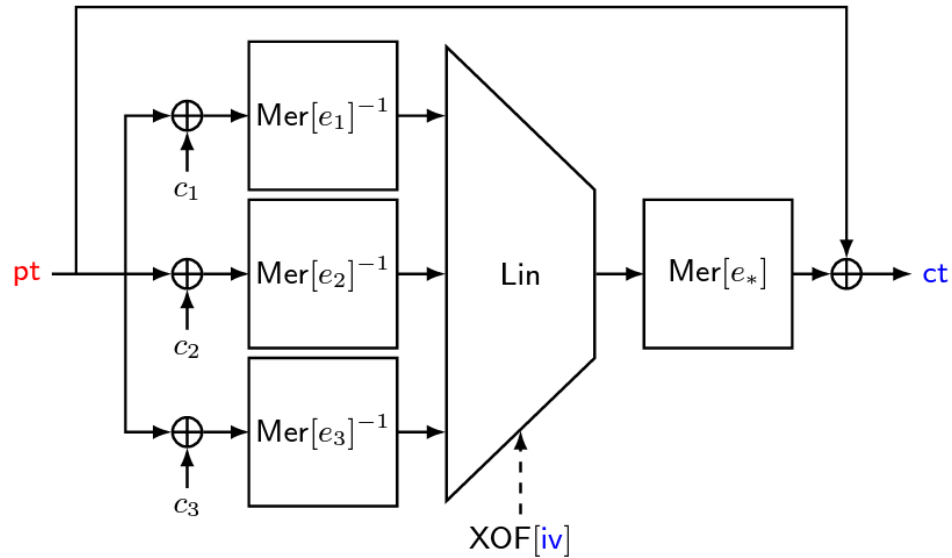


- Let $Mer[e_i](pt) = (pt^d)^{s_i} \cdot pt^{2^{t_i}}$ for some $d \mid 2^n - 1$ and guess the value of pt^d .
- The Mersenne S-boxes are linearized by the guessing.

	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
 - $\text{Mer}[e]^{-1}(x) = x^a$
 - $a = (2^e - 1)^{-1} \bmod (2^n - 1)$
 - 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
 $(x^a)^b$ vs $(x^a + c)^b$

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!

