Magic pot: Algebraic cryptanalysis of full AIM2

Alex Biryukov Pablo García Fernández Aleksei Udovenko

Dagstuhl Seminar 26061, February 3, 2026

DCS and SnT, University of Luxembourg

Work funded by Luxembourg's FNR projects
PQseal (C24/IS/18978392) and CryptoFin (C22/IS/17415825)

Magic Pot a.k.a. Sweet Porridge

Magic Pot a.k.a. Sweet Porridge

AIMer, AIM and AIM2

- `AIMer` is an MPCitH post-quantum signature

AIMer, AIM and AIM2

- `AIMer` is an MPCitH post-quantum signature
- `AIM`/`AIM2`: underlying symmetric-key primitive

AIMer, AIM and AIM2

- `AIMer` is an MPCitH post-quantum signature
- `AIM`/`AIM2`: underlying symmetric-key primitive
- NIST PQC Add. Round 1: `AIMer` v1 (with `AIM`)

AIMer, AIM and AIM2

- `AIMer` is an MPCitH post-quantum signature
- `AIM`/`AIM2`: underlying symmetric-key primitive
- NIST PQC Add. Round 1: `AIMer` v1 (with `AIM`)
- Many attacks:

  [Liu, Mahzoun, Øygarden, and Meier 2023 FSE]
  [Saarinen 2023 pqc-forum]

  [Zhang, Wang, Yu, Guo, and Cui 2023 ASIACRYPT]

  [Yang, Zheng, and Yang 2025 ASIACRYPT]

AIMer, AIM and AIM2

- `AIMer` is an MPCitH post-quantum signature
- `AIM`/`AIM2`: underlying symmetric-key primitive
- NIST PQC Add. Round 1: `AIMer` v1 (with `AIM`)
- Many attacks:

  [Liu, Mahzoun, Øygarden, and Meier 2023 FSE]
  [Saarinen 2023 pqc-forum]
  } Optimized exhaustive search, 13-15 bits reduction

  [Zhang, Wang, Yu, Guo, and Cui 2023 ASIACRYPT]

  [Yang, Zheng, and Yang 2025 ASIACRYPT]

AIMer, AIM and AIM2

- `AIMer` is an MPCitH post-quantum signature
- `AIM`/`AIM2`: underlying symmetric-key primitive
- NIST PQC Add. Round 1: `AIMer` v1 (with `AIM`)
- Many attacks:

  [Liu, Mahzoun, Øygarden, and Meier 2023 FSE]
  [Saarinen 2023 pqc-forum]
  } Optimized exhaustive search, 13-15 bits reduction

  [Zhang, Wang, Yu, Guo, and Cui 2023 ASIACRYPT] Linearization, 2-6 bits

  [Yang, Zheng, and Yang 2025 ASIACRYPT]

AIMer, AIM and AIM2

- `AIMer` is an MPCitH post-quantum signature
- `AIM`/`AIM2`: underlying symmetric-key primitive
- NIST PQC Add. Round 1: `AIMer` v1 (with `AIM`)
- Many attacks:

  [Liu, Mahzoun, Øygarden, and Meier 2023 FSE] } Optimized exhaustive search,
  [Saarinen 2023 pqc-forum] } 13-15 bits reduction

  [Zhang, Wang, Yu, Guo, and Cui 2023 ASIACRYPT] Linearization, 2-6 bits

  [Yang, Zheng, and Yang 2025 ASIACRYPT] Linear layer decomposition + resultants, 14-28 bits

  $\Rightarrow$ eliminated! (October 2024)

AIMer, AIM and AIM2

- `AIMer` is an MPCitH post-quantum signature
- `AIM`/`AIM2`: underlying symmetric-key primitive
- NIST PQC Add. Round 1: `AIMer` v1 (with `AIM`)
- Many attacks:

  [Liu, Mahzoun, Øygarden, and Meier 2023 FSE] } Optimized exhaustive search,
  [Saarinen 2023 pqc-forum] } 13-15 bits reduction

  [Zhang, Wang, Yu, Guo, and Cui 2023 ASIACRYPT] Linearization, 2-6 bits

  [Yang, Zheng, and Yang 2025 ASIACRYPT] Linear layer decomposition + resultants, 14-28 bits

  $\Rightarrow$ eliminated! (October 2024)

- Korean PQC (KpqC): repaired `AIMer` v2 (with `AIM2`)

AIMer, AIM and AIM2

- AIMer is an MPCitH post-quantum signature
- AIM/AIM2: underlying symmetric-key primitive
- NIST PQC Add. Round 1: AIMer v1 (with AIM)
- Many attacks:

  [Liu, Mahzoun, Øygarden, and Meier 2023 FSE]
  [Saarinen 2023 pqc-forum]
  } Optimized exhaustive search, 13-15 bits reduction

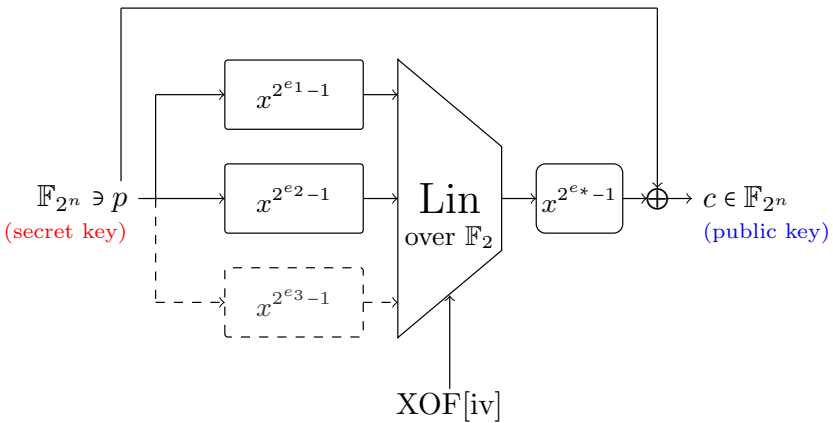
  [Zhang, Wang, Yu, Guo, and Cui 2023 ASIACRYPT] Linearization, 2-6 bits

  [Yang, Zheng, and Yang 2025 ASIACRYPT] Linear layer decomposition + resultants, 14-28 bits

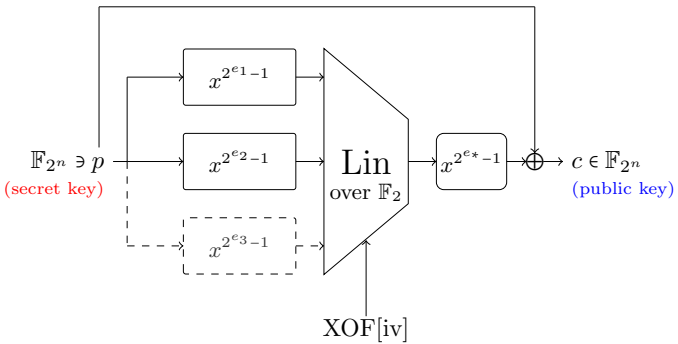
  ⇒ eliminated! (October 2024)

- Korean PQC (KpqC): repaired AIMer v2 (with AIM2)
- ⇒ winner! (January 2025)

AIM1

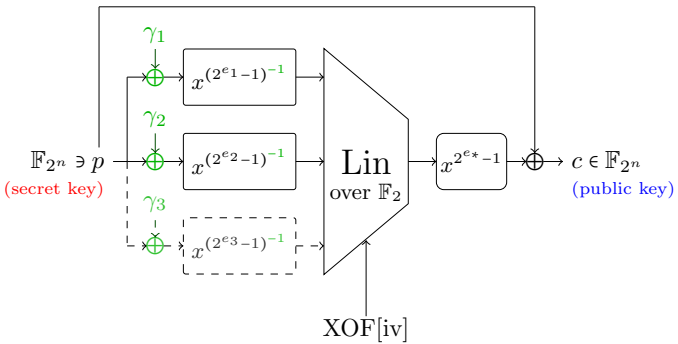

$\mathbb{F}_{2^n} \ni p$
(secret key)
$x^{2^{e_1}-1}$
$x^{2^{e_2}-1}$
$x^{2^{e_3}-1}$
Lin
over $\mathbb{F}_2$
$x^{2^{e_*}-1}$
$c \in \mathbb{F}_{2^n}$
(public key)
XOF[iv]

AIM1



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

AIM2



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

Plan

AIMer, AIM and AIM2

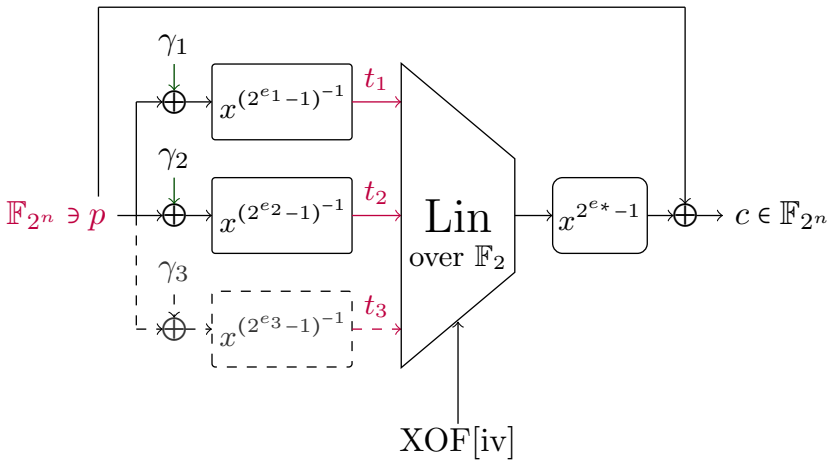
Mixed-order modeling

Path of elimination

Path of determination

Results and conclusions

System of equations (1/2)



System of equations (2/2)

$$(p + \gamma_1)^{(2^{e_1}-1)^{-1}} = t_1$$

System of equations (2/2)

$$(p + \gamma_1) = t_1^{2^{e_1}-1}$$

System of equations (2/2)

$$(p + \gamma_1)t_1 = t_1^{2^{e_1}}$$

System of equations (2/2)

$$\begin{cases} (p+\gamma_1)\cdot t_1 = t_1^{2^{e_1}} \\ (p+\gamma_2)\cdot t_2 = t_2^{2^{e_2}} \\ (p+\gamma_3)\cdot t_3 = t_3^{2^{e_3}} \quad \text{(when } \ell = 3\text{)} \\ (p+c)\cdot \mathrm{Lin}(\mathrm{t}_1,\ldots,\mathrm{t}_\ell) = \mathrm{Lin}(\mathrm{t}_1,\ldots,\mathrm{t}_\ell)^{2^{\mathrm{e}_*}} \end{cases}$$

System of equations (2/2)

$$\begin{cases} (p+\gamma_1)\cdot t_1 = t_1^{2^{e_1}} \\ (p+\gamma_2)\cdot t_2 = t_2^{2^{e_2}} \\ (p+\gamma_3)\cdot t_3 = t_3^{2^{e_3}} \quad \text{(when } \ell = 3\text{)} \\ (p+c)\cdot\left(\lambda_0 + \sum_{i=0}^{n-1}(\lambda_{1,i}t_1^{2^i} + \lambda_{2,i}t_2^{2^i} + \lambda_{3,i}t_3^{2^i})\right) = \left(\lambda_0 + \sum_{i=0}^{n-1}(\lambda_{1,i}t_1^{2^i} + \lambda_{2,i}t_2^{2^i} + \lambda_{3,i}t_3^{2^i})\right)^{2^{e_*}} \end{cases}$$

System of equations (2/2)

$$\begin{cases} (p+\gamma_1)\cdot t_1 = t_1^{2^{e_1}} \\ (p+\gamma_2)\cdot t_2 = t_2^{2^{e_2}} \\ (p+\gamma_3)\cdot t_3 = t_3^{2^{e_3}} \quad \text{(when } \ell = 3\text{)} \\ (p+c)\cdot\left(\lambda_0 + \sum_{i=0}^{n-1}(\lambda_{1,i}t_1^{2^i} + \lambda_{2,i}t_2^{2^i} + \lambda_{3,i}t_3^{2^i})\right) = \left(\lambda_0 + \sum_{i=0}^{n-1}(\lambda_{1,i}t_1^{2^i} + \lambda_{2,i}t_2^{2^i} + \lambda_{3,i}t_3^{2^i})\right)^{2^{e_*}} \end{cases}$$

Monomials: $1,\ t_j^{2^i},\ pt_j^{2^i}$ $(2\ell n + 1$ in total)

Equations: $1 + \ell$ (3 or 4)

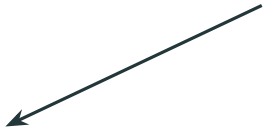
Multiplying equations - Start cooking!

Multiplying equations - Start cooking!

$$(p + \gamma_1)t_1 = t_1^{2^{e_1}}$$

Multiplying equations - Start cooking!

$$(p+\gamma_1)t_1 = t_1^{2^{e_1}}$$



$$(p+\gamma_1)t_1 \times p^j = t_1^{2^{e_1}} \times p^j$$

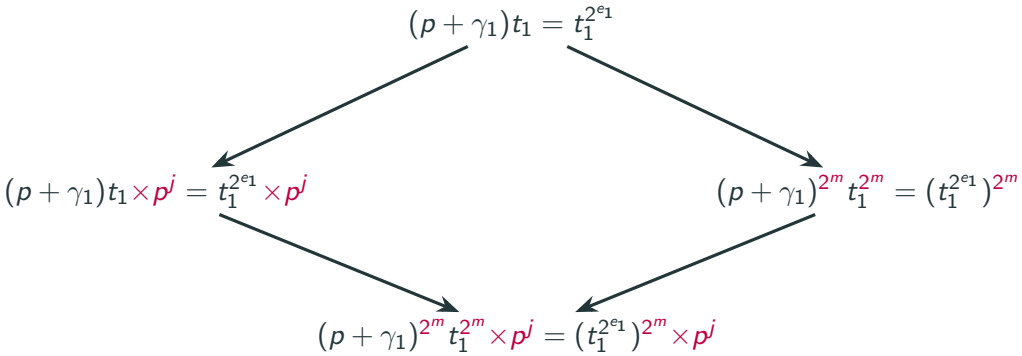
Multiplying equations - Start cooking!

$$(p+\gamma_1)t_1 = t_1^{2^{e_1}}$$

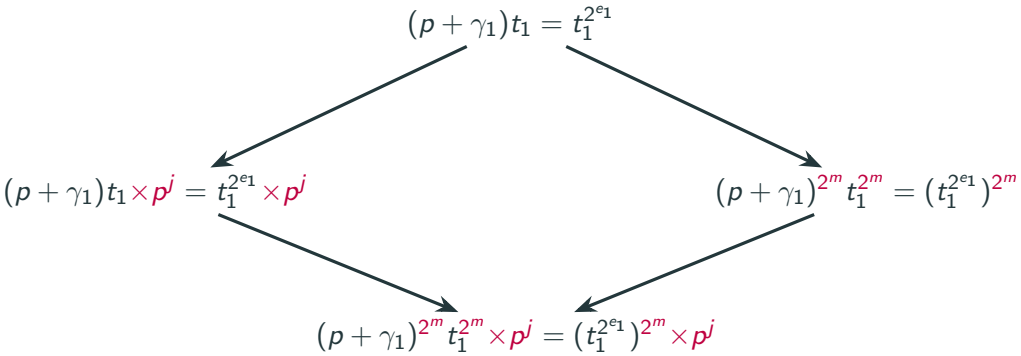
$$(p+\gamma_1)t_1 \times p^j = t_1^{2^{e_1}} \times p^j$$

$$(p+\gamma_1)^{2^m} t_1^{2^m} = (t_1^{2^{e_1}})^{2^m}$$

Multiplying equations - Start cooking!

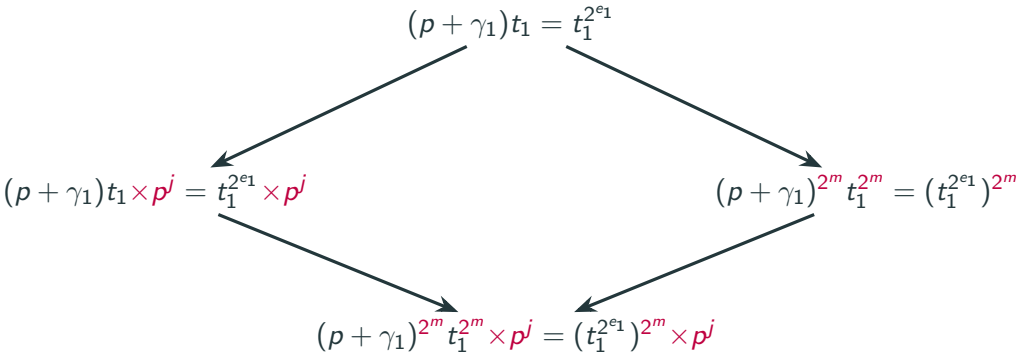


Multiplying equations - Start cooking!



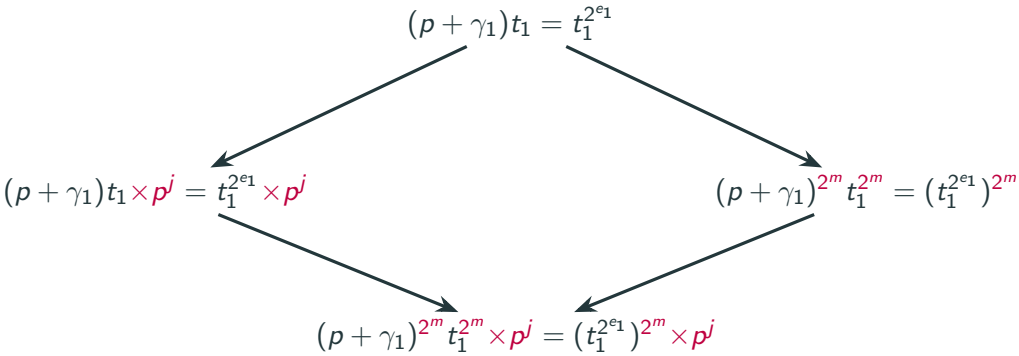
- Monomials $\{1, p, p^2, p^3, \ldots, p^d\} \times \{1, t_1, t_1^2, t_1^4, \ldots, t_1^{2^{n-1}}, t_2, \ldots, t_\ell^{2^{n-1}}\}$

Multiplying equations - Start cooking!



- Monomials $\{1, p, p^2, p^3, \ldots, p^d\} \times \{1, t_1, t_1^2, t_1^4, \ldots, t_1^{2^{n-1}}, t_2, \ldots, t_\ell^{2^{n-1}}\}$
- Set $d = 2^M$, $0 \leq m \leq M$, $0 \leq j \leq 2^M - 2^m$

Multiplying equations - Start cooking!



- Monomials $\{1, p, p^2, p^3, \ldots, p^d\} \times \{1, t_1, t_1^2, t_1^4, \ldots, t_1^{2^{n-1}}, t_2, \ldots, t_\ell^{2^{n-1}}\}$
- Set $d = 2^M$, $0 \leq m \leq M$, $0 \leq j \leq 2^M - 2^m$
- $M = \lceil \frac{\ell}{\ell+1} n \rceil$ ($\frac{2}{3}n$ or $\frac{3}{4}n$) $\Rightarrow$ #equations $\approx$ #monomials

Plan

AIMer, AIM and AIM2

Mixed-order modeling

Path of elimination

Path of determination

Results and conclusions

Sparse linearization (XL)

Question: are all obtained equations useful? (linearly independent)

Sparse linearization (XL)

Question: are all obtained equations useful? (linearly independent)

Experimentally, yes! The system has full rank.

Sparse linearization (XL)

Question: are all obtained equations useful? (linearly independent)

Experimentally, yes! The system has full rank.

Complexity using Wiedemann's method ($\omega = 2$): $\tilde{O}(2^{1.5n})$ for $\ell = 2$ ...

Polynomials

Idea: multiplications by p^j and linear combinations of equations

$\simeq$ multiplications by polynomials $f(p)$

Polynomials

Idea: multiplications by p^j and linear combinations of equations
$\simeq$ multiplications by polynomials $f(p)$

$\Rightarrow$ let's work in $\mathbb{F}_{2^n}[p][t_1, \ldots, t_\ell]$!
(i.e., treat polynomial in p as scalars)[1]

[1] See also [Bariant, Boeuf, Lemoine, Ayala, Øygarden, Perrin, and Raddum 2024 CRYPTO], [Berthomieu, Neiger, and Din 2022 ISSAC]

System of equations

$$
\begin{cases}
(p+\gamma_1)\cdot t_1 = t_1^{2^{e_1}} \\
(p+\gamma_2)\cdot t_2 = t_2^{2^{e_2}} \\
(p+\gamma_3)\cdot t_3 = t_3^{2^{e_3}} \quad \text{(when } \ell = 3\text{)} \\
(p+c)\cdot \mathrm{Lin}(\mathrm{t}_1,\ldots,\mathrm{t}_\ell) = \mathrm{Lin}(\mathrm{t}_1,\ldots,\mathrm{t}_\ell)^{2^{\mathrm{e}_*}}
\end{cases}
$$

System of equations

$$\begin{cases} (p+\gamma_1)^{2^m} \cdot t_1^{2^m} = t_1^{2^{e_1}+2^m} \\ (p+\gamma_2)^{2^m} \cdot t_2^{2^m} = t_2^{2^{e_2}+2^m} \\ (p+\gamma_3)^{2^m} \cdot t_3^{2^m} = t_3^{2^{e_3}+2^m} \quad \text{(when } \ell = 3\text{)} \\ (p+c)^{2^m} \cdot \mathrm{Lin}(\mathrm{t}_1, \ldots, \mathrm{t}_\ell)^{2^{\mathrm{m}}} = \mathrm{Lin}(\mathrm{t}_1, \ldots, \mathrm{t}_\ell)^{2^{\mathrm{e}_*}+2^{\mathrm{m}}} \end{cases}$$

System of equations

$$\begin{cases} (p+\gamma_1)^{2^m} \cdot t_1^{2^m} = t_1^{2^{e_1}+2^m} \\ (p+\gamma_2)^{2^m} \cdot t_2^{2^m} = t_2^{2^{e_2}+2^m} \\ (p+\gamma_3)^{2^m} \cdot t_3^{2^m} = t_3^{2^{e_3}+2^m} \quad \text{(when } \ell = 3\text{)} \\ (p+c)^{2^m} \cdot \mathrm{Lin}(\mathrm{t}_1, \ldots, \mathrm{t}_\ell)^{2^{\mathrm{m}}} = \mathrm{Lin}(\mathrm{t}_1, \ldots, \mathrm{t}_\ell)^{2^{\mathrm{e}*}+2^{\mathrm{m}}} \end{cases}$$

$(\ell+1)M$ equations $(0 \leq m \leq M)$

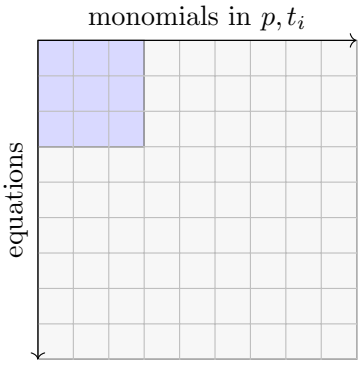
System of equations

$$\begin{cases} (p+\gamma_1)^{2^m} \cdot t_1^{2^m} = t_1^{2^{e_1}+2^m} \\ (p+\gamma_2)^{2^m} \cdot t_2^{2^m} = t_2^{2^{e_2}+2^m} \\ (p+\gamma_3)^{2^m} \cdot t_3^{2^m} = t_3^{2^{e_3}+2^m} \quad \text{(when } \ell = 3\text{)} \\ (p+c)^{2^m} \cdot \mathrm{Lin}(\mathrm{t}_1, \ldots, \mathrm{t}_\ell)^{2^{\mathrm{m}}} = \mathrm{Lin}(\mathrm{t}_1, \ldots, \mathrm{t}_\ell)^{2^{\mathrm{e}_*}+2^{\mathrm{m}}} \end{cases}$$

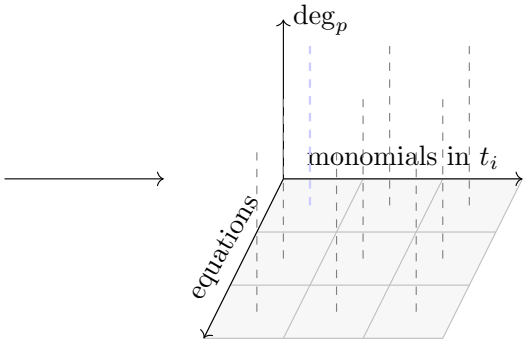
$(\ell+1)M$ equations $(0 \leq m \leq M)$

$\ell n + 1$ monomials $(1,\ t_1,\ t_1^2,\ \ldots,\ t_\ell^{2^{n-1}})$

System of equations



Linearized matrix over $\mathbb{F}_{2^n}$



Linearized matrix over $\mathbb{F}_{2^n}[p]$

Polynomial XL - Stop cooking!

Question: are all obtained equations useful? (linearly independent over $\mathbb{F}_{2^n}[p]$)

Polynomial XL - Stop cooking!

Question: are all obtained equations useful? (linearly independent over $\mathbb{F}_{2^n}[p]$)

- Experimentally, yes! The system has maximum rank.

Polynomial XL - Stop cooking!

Question: are all obtained equations useful? (linearly independent over $\mathbb{F}_{2^n}[p]$)

- Experimentally, yes! The system has maximum rank.
- Sufficient to get full rank at any fixed p!
- For example, $p = 0$ - the constant coefficients matrix ($\ell = 2$):
  - matrix size $(2n + 1) \times (2n + 1)$, over $\mathbb{F}_{2^n}$
  - while degree is exponential ($2^{2n/3}$)

Polynomial XL - Stop cooking!

Question: are all obtained equations useful? (linearly independent over $\mathbb{F}_{2^n}[p]$)

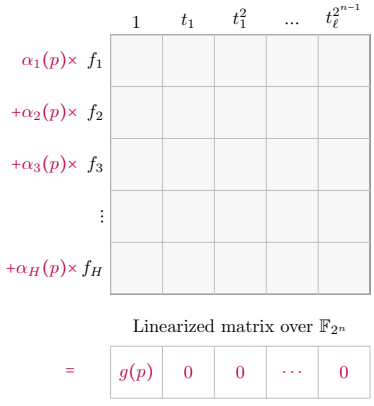
- Experimentally, yes! The system has maximum rank.
- Sufficient to get full rank at any fixed p!
- For example, $p = 0$ - the constant coefficients matrix ($\ell = 2$):
  - matrix size $(2n+1) \times (2n+1)$, over $\mathbb{F}_{2^n}$
  - while degree is exponential ($2^{2n/3}$)
- Provably, also yes! Quite involved, but possible due to structured system.

Solving?

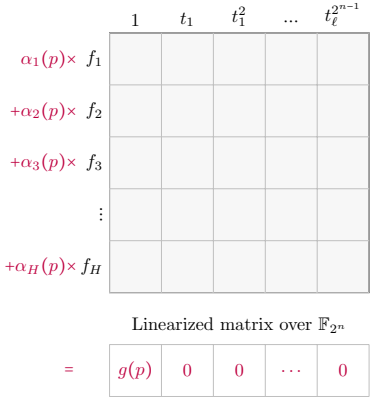
	1	t_1	t_1^2	...	$t_\ell^{2^{n-1}}$
f_1					
f_2					
f_3					
$\vdots$					
f_H					

Linearized matrix over $\mathbb{F}_{2^n}$

Solving?


1
t_1
t_1^2
...
$t_\ell^{2^{n-1}}$
$\alpha_1(p)\times$ f_1
$+\alpha_2(p)\times$ f_2
$+\alpha_3(p)\times$ f_3
$+\alpha_H(p)\times$ f_H
Linearized matrix over $\mathbb{F}_{2^n}$
=
$g(p)$
0
0
$\cdots$
0

Solving?



$\Rightarrow g(p) = 0$, univariate root finding

Solving? Details

- Nullspace basis computation $\tilde{\mathcal{O}}(H^{\omega-1}d)$ [Zhou, Labahn, and Storjohann 2012]

Solving? Details

- Nullspace basis computation $\tilde{\mathcal{O}}(H^{\omega-1}d)$ [Zhou, Labahn, and Storjohann 2012]
- We developed a custom algorithm
  - based on high sparsity
  - HalfGCD is the only involved step (needs FFT)
  - $\Rightarrow$ simpler to implement and analyze
  - state-of-the-art complexity

Solving? Details

- Nullspace basis computation $\tilde{\mathcal{O}}(H^{\omega-1}d)$ [Zhou, Labahn, and Storjohann 2012]
- We developed a custom algorithm
  - based on high sparsity
  - HalfGCD is the only involved step (needs FFT)
  - $\Rightarrow$ simpler to implement and analyze
  - state-of-the-art complexity
- Overall complexity $\approx$ univariate root finding of degree $2^{2n/3}$ ($\ell = 2$)

Plan

AIMer, AIM and AIM2

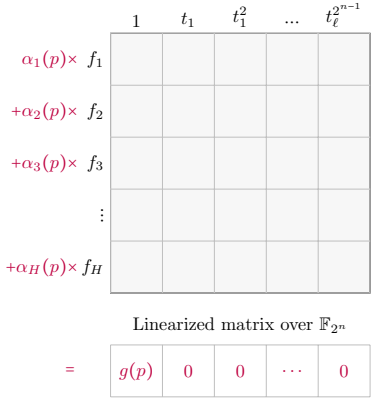
Mixed-order modeling

Path of elimination

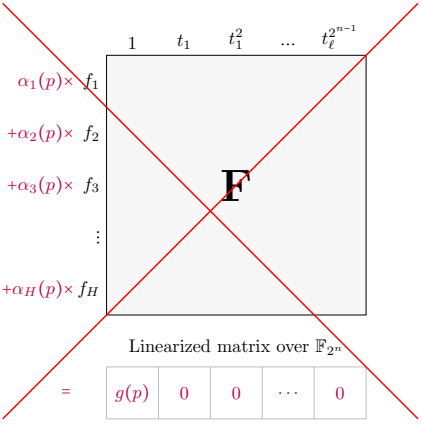
Path of determination

Results and conclusions

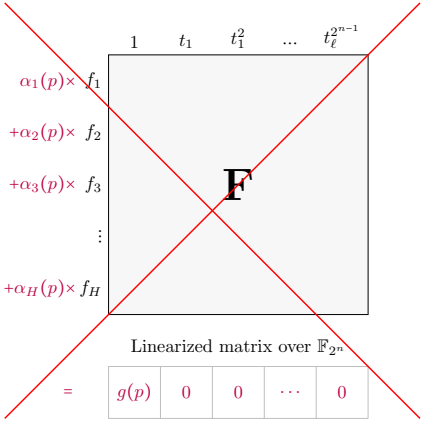
Determination



Determination



Determination



Observation: $g(p)$ divides $\det \mathbf{F}$!!!

Determination process

Consider equation system in $\mathbb{F}[x, y_1, \ldots, y_\ell]$.

Elegant and simple procedure:

1. Write equation system in $\mathbb{F}[x][y_1, \ldots, y_\ell]$

Determination process

Consider equation system in $\mathbb{F}[x, y_1, \ldots, y_\ell]$.

Elegant and simple procedure:

1. Write equation system in $\mathbb{F}[x][y_1, \ldots, y_\ell]$
2. Multiply by monomials in y_i to reach full $\mathbb{F}[x]$-rank (test at $x = 0$)

Determination process

Consider equation system in $\mathbb{F}[x, y_1, \ldots, y_\ell]$.

Elegant and simple procedure:

1. Write equation system in $\mathbb{F}[x][y_1, \ldots, y_\ell]$
2. Multiply by monomials in y_i to reach full $\mathbb{F}[x]$-rank (test at $x = 0$)
3. Compute the determinant $g(x)$ of the equation matrix

Determination process

Consider equation system in $\mathbb{F}[x, y_1, \ldots, y_\ell]$.

Elegant and simple procedure:

1. Write equation system in $\mathbb{F}[x][y_1, \ldots, y_\ell]$
2. Multiply by monomials in y_i to reach full $\mathbb{F}[x]$-rank (test at $x = 0$)
3. Compute the determinant $g(x)$ of the equation matrix
4. Find and test its roots (univariate)!

Determination process

Consider equation system in $\mathbb{F}[x, y_1, \ldots, y_\ell]$.

Elegant and simple procedure:

1. Write equation system in $\mathbb{F}[x][y_1, \ldots, y_\ell]$
2. Multiply by monomials in y_i to reach full $\mathbb{F}[x]$-rank (test at $x = 0$)
3. Compute the determinant $g(x)$ of the equation matrix
4. Find and test its roots (univariate)!

No Gröbner bases, multiplication matrix computations, etc.

Plan

AIMer, AIM and AIM2

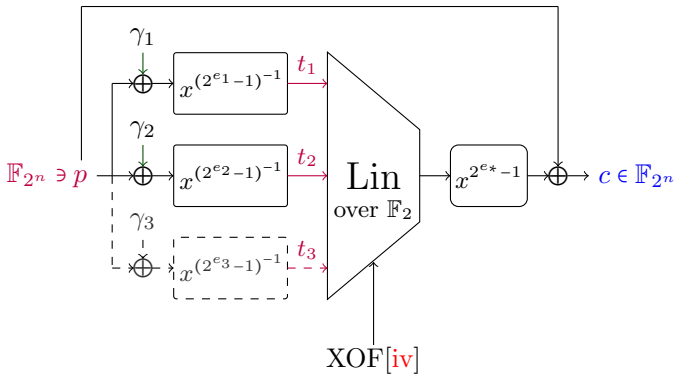
Mixed-order modeling

Path of elimination

Path of determination

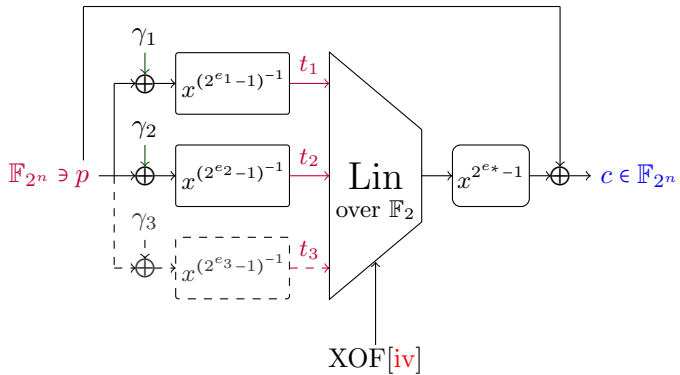
Results and conclusions

Reused-key and related-key models



Extended models for analysis:

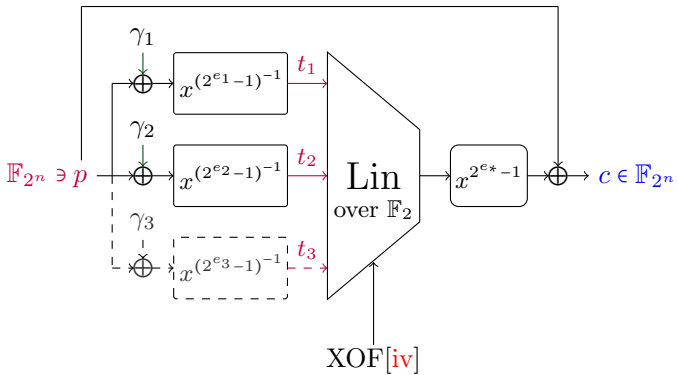
Reused-key and related-key models



Extended models for analysis:

- Reuse key p with different IVs:
  $(p, \mathrm{iv}_1) \to c_1$
  $(p, \mathrm{iv}_2) \to c_1$
  $\vdots$
  $(p, \mathrm{iv}_L) \to c_L$

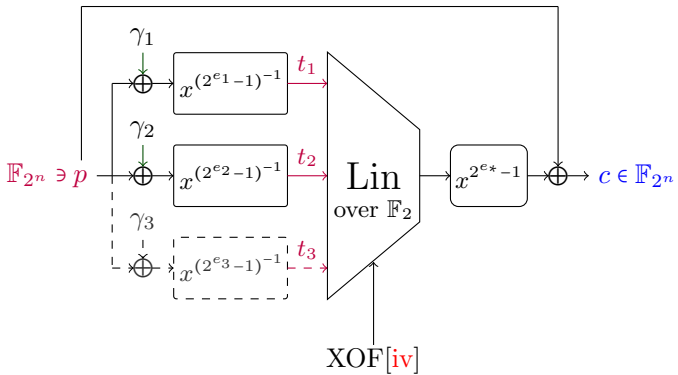
Reused-key and related-key models



Extended models for analysis:

- Reuse key p with different IVs:
- Related-key variant ($\ell = 2$)
  - $(p, \mathrm{iv}_1) \to c_1$
  - $(L(p), \mathrm{iv}_1) \to c_2$
  - $(L^2(p), \mathrm{iv}_1) \to c_3$
  - $(L^3(p), \mathrm{iv}_2) \to c_4$

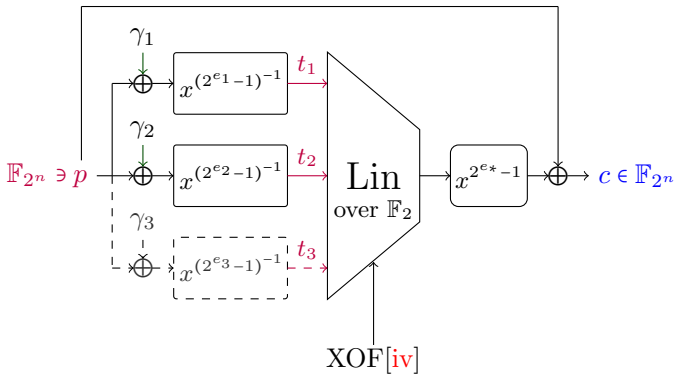
Reused-key and related-key models



Extended models for analysis:

- Reuse key p with different IVs:
- Related-key variant ($\ell = 2$)
- Realistic? Potentially.

Reused-key and related-key models



Extended models for analysis:

- Reuse key p with different IVs:
- Related-key variant ($\ell = 2$)
- Realistic? Potentially.
- Benchmarking and experimental verification!

Cryptanalysis results

Target	n	ℓ	Model	Time (Enc.)	Memory (b)
AIM2-I	128	2	Reuse, 109 IVs	$2^{20.60}$ (3s)	$2^{23.79}$
AIM2-I	128	2	Reuse, 15 IVs	$2^{31.44}$ (1h)	$2^{32.26}$
AIM2-I	128	2	Standard	$2^{103.68}$	$2^{100.33}$

Cryptanalysis results

Target	n	ℓ	Model	Time (Enc.)	Memory (b)
AIM2-I	128	2	Reuse, 109 IVs	$2^{20.60}$ (3s)	$2^{23.79}$
AIM2-I	128	2	Reuse, 15 IVs	$2^{31.44}$ (1h)	$2^{32.26}$
AIM2-I	128	2	Standard	$2^{103.68}$	$2^{100.33}$
AIM2-III	192	2	Reuse, 20 IVs	$2^{35.31}$ (2 days)	$2^{36.22}$
AIM2-III	192	2	Standard	$2^{148.04}$	$2^{144.17}$
AIM2-V	256	3	Reuse, 94 IVs	$2^{29.38}$ (38 min)	$2^{30.34}$
AIM2-V	256	3	Standard	$2^{214.19}$	$2^{209.91}$

Conclusions

Theory

- $\omega = 1$ not impossible!
- new simple and verifiable XL method
- **Q:** relation to Gröbner bases / ideal degree?

Conclusions

Theory

- $\omega = 1$ not impossible!
- new simple and verifiable XL method
- **Q:** relation to Gröbner bases / ideal degree?

Applications

- Cryptanalysis of full AIM2
- 3-round RAIN resists (not linear)
- **Q:** Revisit/simplify previous results?

References i

- Bariant, Augustin, Aurélien Boeuf, Axel Lemoine, Irati Manterola Ayala, Morten Øygarden, Léo Perrin, and Håvard Raddum (Aug. 2024). **"The Algebraic FreeLunch: Efficient Gröbner Basis Attacks Against Arithmetization-Oriented Primitives".** In: *CRYPTO 2024, Part IV*. Ed. by Leonid Reyzin and Douglas Stebila. Vol. 14923. LNCS. Springer, Cham, pp. 139–173. doi: 10.1007/978-3-031-68385-5_5.
- Berthomieu, Jérémy, Vincent Neiger, and Mohab Safey El Din (2022). **"Faster Change of Order Algorithm for Gröbner Bases under Shape and Stability Assumptions".** In: *ISSAC*. ACM, pp. 409–418.

References ii

- Liu, Fukang, Mohammad Mahzoun, Morten Øygarden, and Willi Meier (2023). **"Algebraic Attacks on RAIN and AIM Using Equivalent Representations".** In: *IACR Trans. Symm. Cryptol.* 2023.4, pp. 166–186. doi: 10.46586/tosc.v2023.i4.166-186.
- Saarinen, Markku-Juhani O. (2023). ***Round 1 (Additional Signatures) OFFICIAL COMMENT: AIMer.*** url: https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/BI2ilXblNy0/m/l0Id5TwtAwAJ.

- Yang, Hong-Sen, Qun-Xiong Zheng, and Jing Yang (2025). **"Algebraic Cryptanalysis of AO Primitives Based on Polynomial Decomposition Applications to Rain and Full AIM-I/III/V".** In: *Advances in Cryptology – ASIACRYPT 2025*. Ed. by Goichiro Hanaoka and Bo-Yin Yang. to appear. url: https://ia.cr/2025/981.
- Zhang, Kaiyi, Qingju Wang, Yu Yu, Chun Guo, and Hongrui Cui (Dec. 2023). **"Algebraic Attacks on Round-Reduced Rain and Full AIM-III".** In: *ASIACRYPT 2023, Part III*. Ed. by Jian Guo and Ron Steinfeld. Vol. 14440. LNCS. Springer, Singapore, pp. 285–310. doi: 10.1007/978-981-99-8727-6_10.

 Zhou, Wei, George Labahn, and Arne Storjohann (2012). **"Computing minimal nullspace bases".** In: *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*. ISSAC '12. Grenoble, France: Association for Computing Machinery, 366–373. isbn: 9781450312691. doi: 10.1145/2442829.2442881. url: https://doi.org/10.1145/2442829.2442881.

Further notivation and plan

- Nice compromise between algebraic($\mathbb{F}_2$)/univariate($\mathbb{F}_{2^n}$) degrees/#variables

Further notivation and plan

- Nice compromise between algebraic($\mathbb{F}_2$)/univariate($\mathbb{F}_{2^n}$) degrees/#variables
- Not going fully into $\mathbb{F}_2$, otherwise:
  - Lose sparse structure
  - Hard to analyze/verify/predict system solving over $\mathbb{F}_2$

Further notivation and plan

- Nice compromise between algebraic($\mathbb{F}_2$)/univariate($\mathbb{F}_{2^n}$) degrees/#variables
- Not going fully into $\mathbb{F}_2$, otherwise:
  - Lose sparse structure
  - Hard to analyze/verify/predict system solving over $\mathbb{F}_2$
- Not working fully over $\mathbb{F}_{2^n}$ (Gröbner basis), because:
  - Large univariate degrees (2^{n-1})

Further notivation and plan

- Nice compromise between algebraic($\mathbb{F}_2$)/univariate($\mathbb{F}_{2^n}$) degrees/#variables
- Not going fully into $\mathbb{F}_2$, otherwise:
  - Lose sparse structure
  - Hard to analyze/verify/predict system solving over $\mathbb{F}_2$
- Not working fully over $\mathbb{F}_{2^n}$ (Gröbner basis), because:
  - Large univariate degrees (2^{n-1})

Solution?

Further notivation and plan

- Nice compromise between algebraic($\mathbb{F}_2$)/univariate($\mathbb{F}_{2^n}$) degrees/#variables
- Not going fully into $\mathbb{F}_2$, otherwise:
  - Lose sparse structure
  - Hard to analyze/verify/predict system solving over $\mathbb{F}_2$
- Not working fully over $\mathbb{F}_{2^n}$ (Gröbner basis), because:
  - Large univariate degrees (2^{n-1})

Solution? Ad-hoc mixed-order treatment!

Mixed-ordering

Two interpretations:

- *(Explicit)* Use change of basis

$$(t_i, t_i^2, t_i^4, \ldots, t_i^{2^{n-1}}) \in \mathbb{F}_{2^n}^n \quad \longleftrightarrow \quad (t_{i,0}, t_{i,1}, \ldots, t_{i,n-1}) \in \mathbb{F}_2^n$$

  where $t_{i,j} = \mathrm{Tr}(c_j \cdot t_i)$ is the j-th bit of t_i; follow by (e.g.) Gröbner basis

Mixed-ordering

Two interpretations:

- *(Explicit)* Use change of basis

$$(t_i, t_i^2, t_i^4, \ldots, t_i^{2^{n-1}}) \in \mathbb{F}_{2^n}^n \quad \longleftrightarrow \quad (t_{i,0}, t_{i,1}, \ldots, t_{i,n-1}) \in \mathbb{F}_2^n$$

  where $t_{i,j} = \mathrm{Tr}(c_j \cdot t_i)$ is the j-th bit of t_i; follow by (e.g.) Gröbner basis

- *(Implicit)* Manage the degrees by careful choice of multiplications/squarings:
  - degree in p at most d as integer
  - algebraic degree in $(t_1, t_2, \ldots, t_\ell)$ at most 1
  - $\Rightarrow$ monomial set $\{1, p, p^2, p^3, \ldots, p^d\} \otimes \{1, t_1, {t_1}^2, {t_1}^4, \ldots, {t_1}^{2^{n-1}}, t_2, \ldots, {t_\ell}^{2^{n-1}}\}$