

AEAD-MODE MXP – BEYOND THE BIRTHDAY BOUND WITHOUT LOSS OF EFFICIENCY

VITALY KIRYUKHIN

LLC “SFB Lab”, JSC “InfoTeCS”

CTCrypt 2025

4 June 2025

vitaly.kiryukhin@sfblaboratory.ru



AUTHENTICATED ENCRYPTION WITH ASSOCIATED DATA

Input:

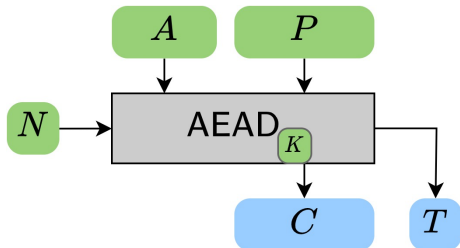
- Secret key K
- Nonce N
- Associated data (header) A
- Plaintext P

Output:

- Ciphertext C
- Tag T

Security properties:

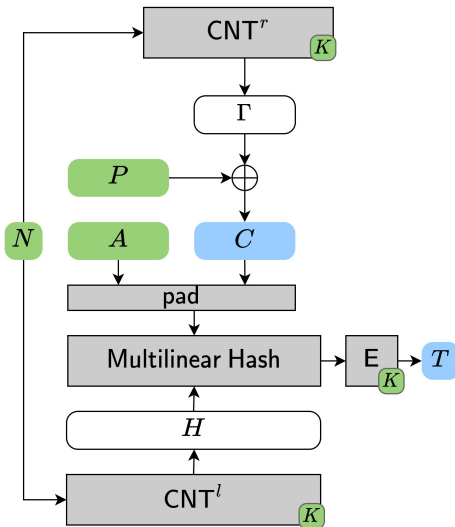
- confidentiality of plaintext P
- integrity of packet (N, A, C, T)



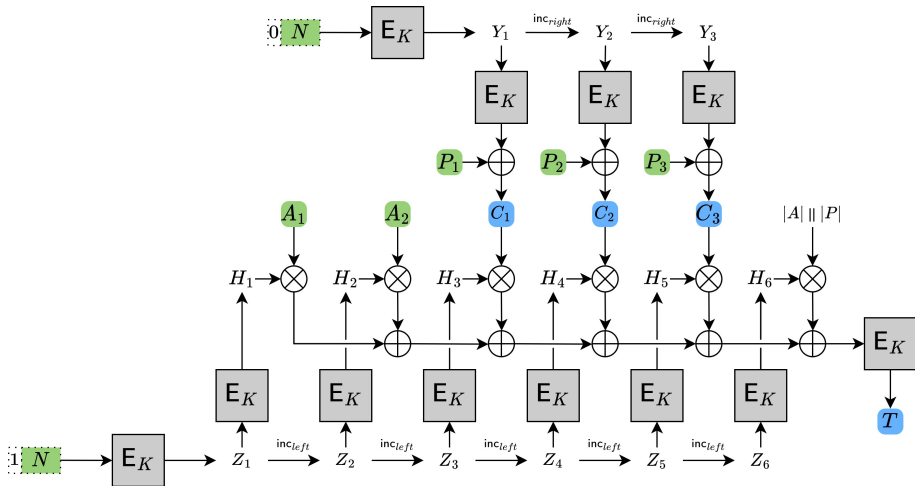
STANDARDIZED AEAD-MODE MGM

GOST 34.13-2018 Alteration №1
MGM – Multilinear Galois Mode

- CNT for encryption
- CNT for hash function key
- Hash-then-encrypt MAC
- One-time hash function key
- Multilinear hash



MGM: EXAMPLE $a = 2, p = 3$



SOME HISTORY NOTES: MGM ON CTCRYPT

- 2017 [Nozdrunov]
 - Prototype of MGM: **PD-mode**
- 2019 [Kurochkin, Fomin]
 - Birthday attacks on integrity of MGM
- 2021 [Akhmetzyanova, Alekseev, Babueva, Bozhko, Smyshlyaev]
 - AEAD-mode **MGM2**: CTR, domain separation, misuse resistance
- 2022 [Akhmetzyanova, Alekseev, Babueva, Bozhko, Smyshlyaev]
 - AEAD-mode **sMGM**: SIV, ACPKM and other features
- 2024 [Kiryukhin]
 - Pseudorandom functions **MGM-PRF**, **MGM2-PRF**, **SUM-MGM**
- 2025 [Kiryukhin]
 - AEAD-mode **MXP**

OUR GOAL

PROBLEM

MGM is secure only up to **birthday bound**.

No more than $2^{\frac{n}{2}}$ blocks can be protected with one key.

1. Restriction from “provable security”
2. CTR-like attacks on confidentiality
3. Attacks on integrity [Kurochkin, Fomin – CTCrypt 2019]

MGM is secure only up to **birthday bound**.

No more than $2^{\frac{n}{2}}$ blocks can be protected with one key.

1. Restriction from “provable security”
2. CTR-like attacks on confidentiality
3. Attacks on integrity [Kurochkin, Fomin – CTCrypt 2019]

EXAMPLE

MGM with block cipher “Magma” ($n = 64$) and $\pi_{\text{enc}} = \pi_{\text{mac}} = 2^{-10}$.

No more than 2^{26} blocks (512 MB) with a single key.

NOTE ABOUT PERFORMANCE AND SECURITY

Kuznyechik (128-bit) is much more **secure** than Magma (64-bit),
but at the same time, Magma is:

- **no slower** on any platform;
- **much faster** in a **low-resource** environment;

and also multiplication in $GF(2^n)$ is:

- **comparable** to encryption;
- **much faster** in many cases.

New AEAD-mode:

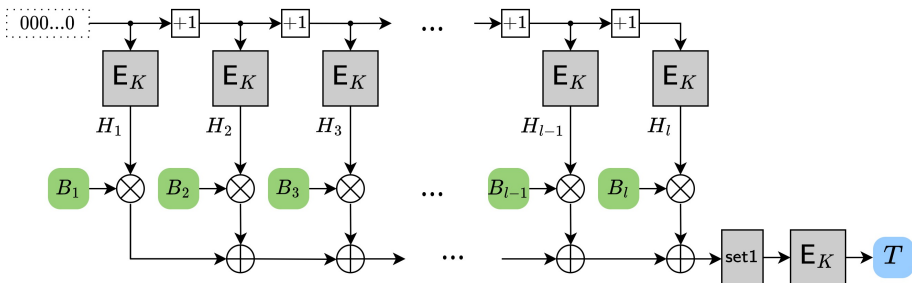
- has at least **the same performance** as MGM
- has key capacity that is way **beyond the birthday bound** (BBB)
 - acceptable security level with low-resource ciphers
- inherits all good properties of MGM:
 - one cipher key
 - parallelism
 - online processing
 - inverse-free
 - nonce-misuse integrity

AEAD-MODE MXP: MULTILINEAR MODE AND XOR OF PERMUTATION

MXP IS COMBINATION OF TWO PRFs

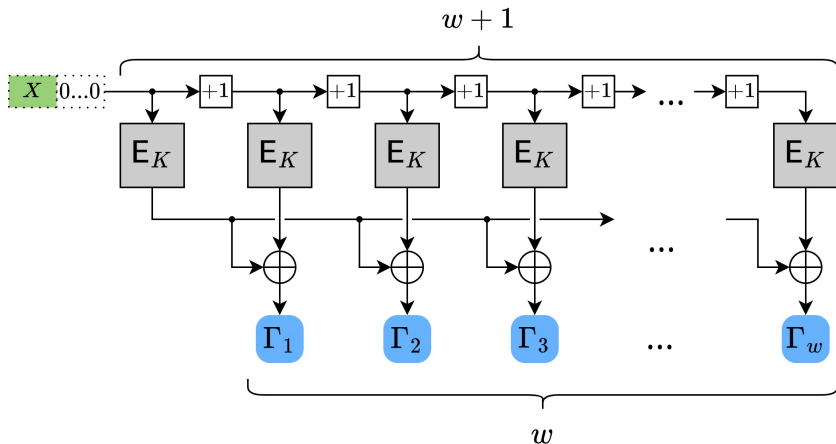
- MGM2-PRF – multilinear hash then encryption
- XORP – Xor of Permutation

MGM2-PRF [KIRYUKHIN – CTCRYPT 2024]



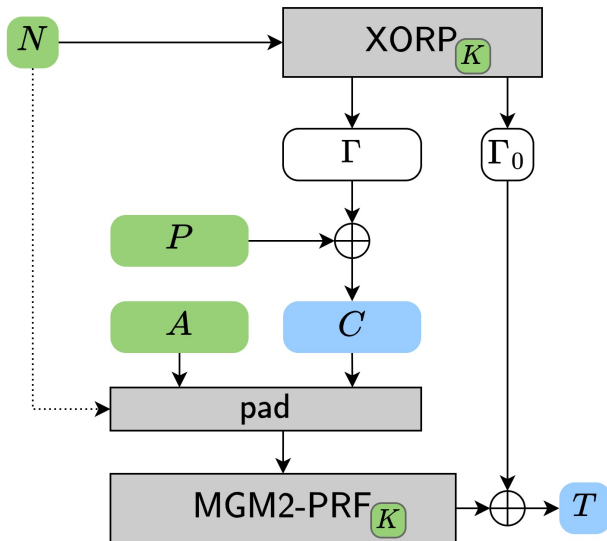
- PRF-security up to birthday bound
- Great as almost-universal hash
 - “ideal” collision probability $\approx 2^{-n}$ for any ℓ
- ℓ -block key $H = (H_1, \dots, H_\ell)$ can be precomputed
- Message $(B_1, \dots, B_\ell)$ is injectively padded

XORP [IWATA – FSE 2006]

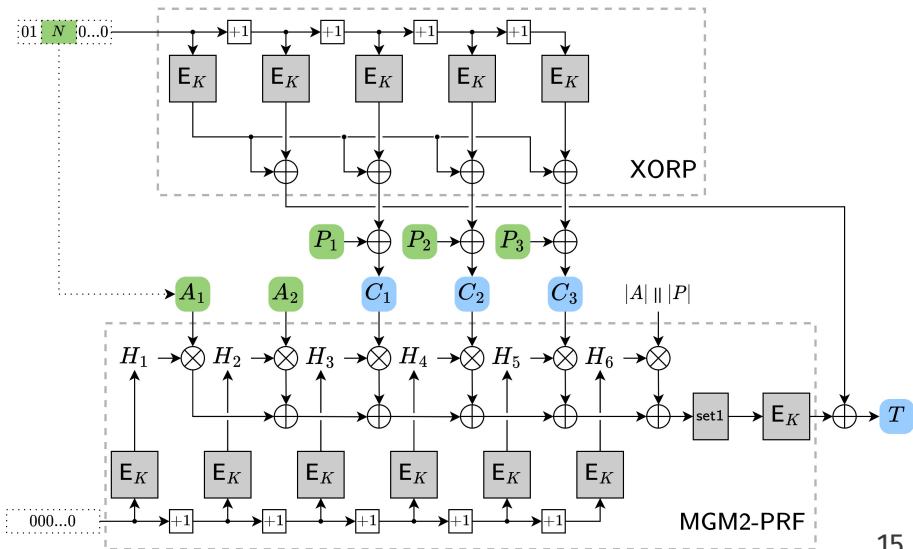


- Almost optimal security: up to $2^n/w$ processed blocks
- Tiny overhead: $(w + 1)$ encryptions per w outputs

MXP: MGM2-PRF AND XORP WITH THE SAME KEY



MXP: EXAMPLE $a = 2, p = 3$



MXPk2 is the same as MXP,

but the MGM2-PRF key is generated from the master key K ,

$$K_{\text{MGM2-PRF}} = \text{XORP}^w(K, \text{const}), \quad w = \frac{k}{n},$$

$$K_{\text{XORP}} = K.$$

SYNTHESIS

DOMAIN SEPARATION

Hash inside MGM2-PRF	1...
Counters of XORP	01...
Key derivation in MXPk2	001...
Nonce hiding	0001...
Reserved	...
Counters in MGM2-PRF	00000000...

MXP

Domain separation simplifies analysis and is cost-neutral.

МХР

Keystream is produced with a single call to XORP.

- XORP is well studied
- tiny overhead
- BBB-security
- long packets require *many* XORP calls (MXPL mode),
but here we assume short packets

COMPARISON

	Polynomial	Multilinear
Examples	GCM, Poly1305	MGM, MXP
Key length	one block	ℓ blocks
Degradation	linear	almost none
Effective tag length	$n - \log_2(\ell)$	n

COMPARISON

	Polynomial	Multilinear
Examples	GCM, Poly1305	MGM, MXP
Key length	one block	ℓ blocks
Degradation	linear	almost none
Effective tag length	$n - \log_2(\ell)$	n

MXP

We need full-block tags $\Rightarrow$ multilinear hash.

With precomputations both constructions have similar performance.

COMPARISON

	Polynomial	Multilinear
Examples	GCM, Poly1305	MGM, MXP
Key length	one block	ℓ blocks
Degradation	linear	almost none
Effective tag length	$n - \log_2(\ell)$	n

MXP

We need full-block tags $\Rightarrow$ multilinear hash.

With precomputations both constructions have similar performance.

PXP

If short tags ($\approx n/2$ bits) are allowed,
a polynomial hash is preferred.

HASH FUNCTION KEY

COMPARISON

	Onetime	Longterm
Examples	MGM, MGM2	MXP
BBB-security proof	No	Yes
Precomputations	No	Yes
Sidechannel leakage	?	?

MXP

⇒ Longterm key for hash function.

1. GCM – hash-then-mask:
 - simple, but fragile if the nonce is reused

1. GCM – hash-then-mask:
 - simple, but fragile if the nonce is reused
2. MGM – hash-then-encrypt:
 - birthday paradox limitations

1. GCM – hash-then-mask:
 - simple, but fragile if the nonce is reused
2. MGM – hash-then-encrypt:
 - birthday paradox limitations
3. MXP – hash-then-encrypt-then-mask:

Nonces	Unique	Reused
MGM2-PRF role	Almost universal hash	PRF-as-MAC
Security	BBB	up to BB

- Structure:

block		
flag	nonce	block counter
01	N	00..0
2	s	$n - s - 2$

- The nonce length s is parametric
- We recommend to use counter as nonce
- Random nonces give low-level security
- Nonce is optionally included in header

Optionally, nonce can be *hidden* with the same key K .

Similarly to HN1-transform

$$\tilde{N} = N \oplus \text{msb}_s(E_K(0001 || \text{msb}_{n-4}(C_1)) \oplus E_K(0001 || \text{msb}_{n-4}(C_2))).$$



BELLARE M., NG R., TACKMANN B.

NONCES ARE NOTICED: AEAD REVISITED

CRYPTO 2019

PERFORMANCE

	#E	# $\otimes$	
GCM	$2 + p$	$a + p + 1$	
MGM	$4 + a + 2p$	$a + p + 1$	
MGM2	$2 + a + 2p$	$a + p + 1$	
MXP	$4 + a + 2p$	$a + p + 1$	no precomputations
	$3 + p$	$a + p + 1$	precomputations
	$3 + p$	$p + 1$	+ fixed header

a blocks in header A , p blocks in plaintext P , $a > 0$, $p > 0$

SECURITY ANALYSIS

KNOWN RESULTS: BOTH PRF ARE SECURE

THEOREM

$$\text{Adv}_{\text{XORP}^w[\Pi]}^{\text{PRF}}(\infty, q) \leq \frac{q \cdot w}{2^n} + \frac{q \cdot w^2}{2^{n+1}}.$$

[Cogliati, Dutta, Nandi, Patarin, Saha – EUROCRYPT 2023]

THEOREM

$$\text{Adv}_{\text{MGM2-PRF}[\Pi]}^{\text{PRF}}(\infty, q, \ell) \leq \frac{q \cdot (q - 1)}{2^{n+1}} + \frac{q \cdot (q - 1)}{2^n - q - \ell + 1} \leq \frac{5q^2 - q}{2^{n+1}}.$$

[Kiryukhin – CTRcrypt 2024]

1. MGM2-PRF and XORP are good secure PRFs when used with **two independent keys**, but MXP uses a **single** encryption key...

1. MGM2-PRF and XORP are good secure PRFs when used with **two independent keys**, but MXP uses a **single** encryption key...
2. PRP-PRF Switching Lemma gives a trivial result here...

1. MGM2-PRF and XORP are good secure PRFs when used with **two independent keys**, but MXP uses a **single** encryption key...
2. PRP-PRF Switching Lemma gives a trivial result here...

By using H-coefficients technique,
we have proven that such usage is also secure!

THEOREM (XORP WITH EXTERNAL KEY USAGE)

The distinguishing advantage between $(\text{XORP}[\Pi], \Pi)$ and (R, Π) under domain separation,

$$\text{Adv}_{\text{XORP}[\Pi]}^{\text{PRF-EKU}}(\infty, q, r) \leq \underbrace{\frac{2q^3\tilde{w}^4}{3 \cdot 2^{2n}} + \frac{2q\tilde{w}^2r^2}{2^{2n}} + \frac{2q^2r\tilde{w}^3}{2^{2n}}}_{\text{cost of external usage}} + \frac{qw}{2^n} + \frac{qw^2}{2^{n+1}},$$

q – queries to $O \in \{\text{XORP}[\Pi], R\}$,

r – queries to Π (external usage),

w – width of XORP,

n – block bit size,

$(q\tilde{w}^2 + r\tilde{w}) \leq 2^n$, $\tilde{w} = w + 1$.

THEOREM (SECURITY OF MXP AND MXPk2)

$$\begin{aligned} \text{Adv}_{\text{MXP}[E]}^{\text{NAE}}(t, q, v, a, p) &\leq \\ &\leq \text{Adv}_E^{\text{PRP}}(\tilde{t}, \sigma) + \text{Adv}_{\text{XORP}^{p+1}[\Pi]}^{\text{PRF-EKU}}(\infty, \tilde{q}, \ell + \tilde{q}) + v \cdot \text{Adv}_{\text{MGM2-PRF}[\Pi]}^{\text{AXU}}(\ell), \\ \text{Adv}_{\text{MXPk2}[E]}^{\text{NAE}}(t, q, v, a, p) &\leq \\ &\leq 2 \cdot \text{Adv}_E^{\text{PRP}}(\tilde{t}, \sigma) + \text{Adv}_{\text{XORP}^{p+1}[\Pi]}^{\text{PRF}}(\infty, \tilde{q} + 1) + v \cdot \text{Adv}_{\text{MGM2-PRF}[\Pi]}^{\text{AXU}}(\ell), \end{aligned}$$

- q protected packets, v forgery attempts, $\tilde{q} = q + v$ queries,
- a and p – length of header and plaintext,
- $\ell = (a + p + 1)$ – packet length in blocks,
- $\sigma = \ell + \tilde{q}(p + 3)$ – block cipher input/output pairs,
- $\tilde{t} = t + \sigma \approx t$ – computation resources.

THEOREM (MRAE-INT SECURITY OF MXP)

The probability of forge new (N, A, C, T) in nonce-misuse setting,

$$\begin{aligned} \text{Adv}_{\text{MXP}[E]}^{\text{MRAE-int}}(t, q, v, a, p) &\leq \\ &\leq \text{Adv}_E^{\text{PRP}}(\tilde{t}, \sigma) + \text{Adv}_{\text{XORP}^{p+1}[\Pi]}^{\text{PRF-EKU}}(\infty, \tilde{q}, l + \tilde{q}) + \text{Adv}_{\text{MGM2-PRF}[\Pi]}^{\text{PRF}}(\infty, \tilde{q}, l) + \frac{v}{2^\tau}, \end{aligned}$$

$\tau \leq n$ is a tag length.

If nonce is NOT included in header, then the forge is new (A, C) .

$\Rightarrow$ MXP provides integrity (but not confidentiality) protection even if nonces are reused.

$$\text{Adv}_{\text{MXP}[E]}^{\text{NAE}}(t, q, v, a, p) \lesssim \frac{q \cdot \ell^2}{2^{n+1}} + \frac{2 \cdot q^3 \cdot \ell^4}{3 \cdot 2^{2n}},$$

$$\text{Adv}_{\text{MXPk2}[E]}^{\text{NAE}}(t, q, v, a, p) \lesssim \frac{q \cdot \ell^2}{2^{n+1}},$$

where:

- q protected packets,
- v forgery attempts ($v \ll q$),
- a blocks in header,
- p blocks in plaintext,
- $\ell \leq a + p + 1$ blocks in packet,
- n bits in block.

EXAMPLE

- “Magma” ($n = 64$)
- short-length packets, $\ell \leq 2^7$ blocks
- security level $\pi_{\text{enc}} = \pi_{\text{mac}} = 2^{-10}$
- tags are not truncated
- forgery attempts are negligible $v \ll q$

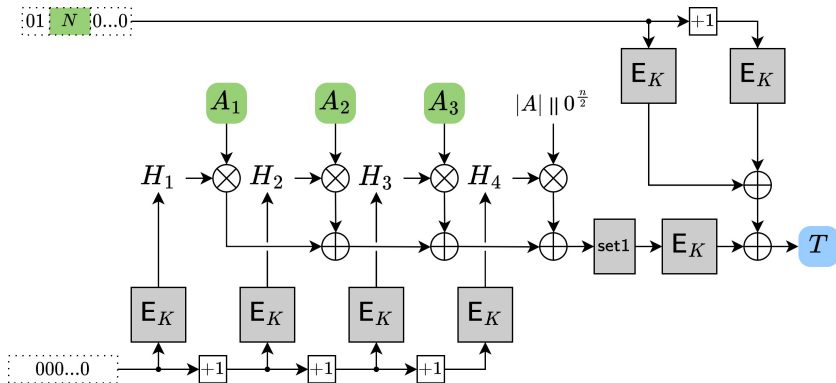
EXAMPLE

- “Magma” ($n = 64$)
- short-length packets, $\ell \leq 2^7$ blocks
- security level $\pi_{\text{enc}} = \pi_{\text{mac}} = 2^{-10}$
- tags are not truncated
- forgery attempts are negligible $v \ll q$

KEY CAPACITY

	MGM	MXP	MXPk2
Packets (q)	2^{19}	2^{30}	2^{40}
Blocks ($q\ell$)	2^{26}	2^{37}	2^{47}

MXP AS “ONLY MAC” MODE: EXAMPLE $a = 3, p = 0$



Performance with precomputation:

- 3 encryptions
- $(a + 1)$ multiplications

“ONLY MAC” MODE: HEURISTIC BOUNDS

$$\text{Adv}_{\text{MXP}[E]}^{\text{NAE}}(t, q, v, a, 0) \lesssim \frac{35q^3 + 24q\ell^2 + 16q^2\ell}{2^{2n}} + \frac{q}{2^n},$$

$$\text{Adv}_{\text{MXPk2}[E]}^{\text{NAE}}(t, q, v, a, 0) \lesssim \frac{q \cdot w^2}{2^{n+1}}, \quad w = \frac{k}{n},$$

where:

- q protected packets,
- v forgery attempts ($v \ll q$),
- a blocks in header, $\ell = a + 1$,
- $p = 0$ blocks in plaintext,
- n bits in block.

“ONLY MAC” MODE: EXAMPLE

- “Magma” ($n = 64$)
- security level $\pi_{\text{enc}} = \pi_{\text{mac}} = 2^{-10}$
- tags are not truncated
- forgery attempts are negligible $v \ll q$
- padding procedure is slightly modified ($a > 2^{n/2}$)

“ONLY MAC” MODE: EXAMPLE

- “Magma” ($n = 64$)
- security level $\pi_{\text{enc}} = \pi_{\text{mac}} = 2^{-10}$
- tags are not truncated
- forgery attempts are negligible $v \ll q$
- padding procedure is slightly modified ($a > 2^{n/2}$)

KEY CAPACITY IN “ONLY MAC” MODE

	MGM	MXP	MXPk2
Packets (q)	2^{13}	2^{37}	2^{50}
Length (ℓ)	2^{13}	2^{37}	2^{62}
Blocks ($q\ell$)	2^{26}	2^{74}	2^{112}

Asymptotically, from $2^{\frac{n}{2}}$ to 2^{2n} blocks!

ATTACKS

ATTACKS ON MXP AND MXPk2

- Confidentiality: CTR-like attack “over a single packet”
- Integrity: tag guessing
- Integrity with reused nonce: birthday attack on MGM2-PRF

ATTACKS ON MXP AND MXPk2

- Confidentiality: CTR-like attack “over a single packet”
- Integrity: tag guessing
- Integrity with reused nonce: birthday attack on MGM2-PRF

FACT 1

Security bounds of MXPk2 are tight.

Security bounds of MXP are NOT tight.

HYPOTHESIS 1

MXP is **more secure** than currently proven.

Security bounds of MXP and MXPk2 is almost **equal**.

FACT 2

MXP is as secure against key recovery as the block cipher itself.

FACT 2

MXP is as secure against key recovery as the block cipher itself.

HYPOTHESIS 2

For many ciphers MXP is **more secure** than cipher itself:

- The attacker does not see any input-output pairs of the cipher
- The cost of non-trivial attacks increases by 2^n due to the XORP mask guessing
- In nonce-misuse setting, input-output pairs can be obtained only after birthday paradox ($q \gtrapprox 2^{\frac{n}{2}}$)

KEY RECOVERY ATTACKS ON “MAGMA”

<i>Mode</i>	<i>Applicability of “Fixed point” and “Reflection” attacks</i>
MGM2 and CTR	immediately
MGM	after birthday paradox or with low-probability
MXP (nonce-misusing)	after birthday paradox
MXP (nonce-respecting)	hypothesis: inapplicable

COMPARISON WITH OTHER BBB-AEAD

BBB-AEAD based on block ciphers:

- CHM [Iwata – FSE 2006]
- CIP [Iwata – AFRICACRYPT 2008]
- XOCB [Bao, Hwang, Inoue, et al. – EUROCRYPT 2023]
- eGCM [Chung, Hwang, Kim, et al. – EUROCRYPT 2025]

COMPARISON WITH OTHER BBB-AEAD

CHM / CIP

- XORP-based
- CHM uses polynomial hash and “hash-then-mask”
- CIP uses two keys and applies MH to fragments

XOCB

- $(a + p + 8)$ encryptions per packet
- isn't inverse-free
- isn't MRAE-int secure
- has fragile integrity protection

⇒ MXP provides much stronger integrity and security in MRAE-int

eGCM [CHUNG, HWANG, KIM, ET AL. – EUROCRYPT 2025]

- “masked” enhanced XORP with two secret counters
- 2 block cipher keys and 3 hash keys
- arbitrary nonce length
- “hash-then-mask” paradigm
- hash function is not specified, but polynomial hash is assumed
- no MRAE-int security
- eGCM-SIV is MRAE-secure, but it is not online-scheme

⇒ Direct comparison with MXP is difficult

CONCLUSION

- New AEAD-mode
 - MXP: Multilinear mode and Xor of Permutation

CONCLUSION

- New AEAD-mode
 - MXP: Multilinear mode and Xor of Permutation
- Performance:
 - same as with MGM
 - much faster than MGM with precomputation

- New AEAD-mode
 - MXP: Multilinear mode and Xor of Permutation
- Performance:
 - same as with MGM
 - much faster than MGM with precomputation
- Beyond the birthday bound (BBB) security
 - up to $2^{\frac{2}{3}n}$ encrypted blocks with a single key
 - up to $2^{\frac{4}{3}n}$ protected blocks in “only MAC” mode

- New AEAD-mode
 - MXP: Multilinear mode and Xor of Permutation
- Performance:
 - same as with MGM
 - much faster than MGM with precomputation
- Beyond the birthday bound (BBB) security
 - up to $2^{\frac{2}{3}n}$ encrypted blocks with a single key
 - up to $2^{\frac{4}{3}n}$ protected blocks in “only MAC” mode
- Integrity in nonce-misuse setting and other good features of MGM

Hypothesis 1: MXP is **more secure** than currently proven:

- up to $2^n/\ell$ encrypted blocks with a single key
- up to 2^{2n} protected blocks in “only MAC” mode

Hypothesis 2:

- nontrivial key recovery attacks are inapplicable to MXP-Magma

Thank you for attention!
Questions?

VITALY KIRYUKHIN

LLC "SFB Lab", JSC "InfoTeCS"

CTCrypt 2025

4 June 2025

vitaly.kiryukhin@sfblaboratory.ru



WHY DO WE NEED BBB-MODES IF THERE IS AN EXTERNAL RE-KEYING?

Usually, the probability of a threat is computed for **one specific** key
⇒ an external re-keying solves all problems

WHY DO WE NEED BBB-MODES IF THERE IS AN EXTERNAL RE-KEYING?

Usually, the probability of a threat is computed for **one specific** key
⇒ an external re-keying solves all problems

Multi-user (multi-key) setting:

- μ independent secret keys (users)
- Forgery/threat for **any** one of μ users
- The success probability **increases linearly** with μ

WHY DO WE NEED BBB-MODES IF THERE IS AN EXTERNAL RE-KEYING?

Example:

- μ independent secret keys
- each key protects $q = 2^{10}$ packets with $\ell = 2^4$ blocks
- total $\mu \cdot q$ packets and $\mu \cdot q \cdot \ell$ blocks
- the probability of attack must be less than 2^{-10}

WHY DO WE NEED BBB-MODES IF THERE IS AN EXTERNAL RE-KEYING?

Example:

- μ independent secret keys
- each key protects $q = 2^{10}$ packets with $\ell = 2^4$ blocks
- total $\mu \cdot q$ packets and $\mu \cdot q \cdot \ell$ blocks
- the probability of attack must be less than 2^{-10}

How much data can be protected in total?

	$\text{Adv}(q, \ell)$	μ	$\mu \cdot \text{Adv}(q, \ell)$	$\mu \cdot q \cdot \ell$
MGM	2^{-35}	2^{25}	2^{-10}	2^{39}
MXP	2^{-46}	2^{36}		2^{50}

WHY DO WE NEED BBB-MODES IF THERE IS AN EXTERNAL RE-KEYING?

⇒ If a multi-user (multi-key) threat model is used,
then we must apply at least one of the following:

- strict limitation of the total key capacity
- Kuznyechik
- BBB-secure cipher modes