# Research Statement

## Kushankur Dutta

*Ph.D. Student, IAI, TCG CREST*


# 1 Coursework

(a) Courses at First Semester

| Course | Grade |
|---|---|
| Discrete Mathematics | 90/100 |
| Cryptology-I | 86/100 |
| Automata & Formal Lang. | 74/100 |
| AIML | 89/100 |

(b) Courses at Second Semester

| Course | Grade |
|---|---|
| Advanced Cryptology | 73/100 |
| Quantum Information & Cryptology | 71/100 |
| Design & Analysis Of Algorithm | 82/100 |
| Research Methodology | 74/100 |

# 2 Research Done

Currently my research works are focused on symmetric key cryptography, specially provable security. My primary problems are based on Message Authentication Code or MAC (a type of signature), where providing higher security of MAC against adversaries, is the goal. We are trying to optimize security bounds of a few constructions like EWCDM[1], EDM[2], LightMAC[3], SoEM2[4] and their other variants.

## 2.1 Security bound improvement of EWCDM and DWCDM

In CRYPTO'16, Cogliati and Seurin proposed a nonce based MAC, called Encrypted Wegman-Carter with Davies-Meyer (EWCDM) [1] , that gives 2n/3-bit MAC security in nonce respecting adversary. This construction used two independent block cipher keys. In CRYPTO'18, Datta et al. came up with a single-keyed block cipher based variant of EWCDM, called Decrypted Wegman-Carter with Davies-Meyer (DWCDM) [5]. That also provides 2n/3-bit MAC security, when nonce space is restricted to 2n/3 bit.

We have improved the MAC security of EWCDM from 2n/3 bit MAC security to 3n/4 bit. As well the security of DWCDM has been improved from 2n/3 bit MAC security to 3n/4, when the nonce space is extended to 3n/4 bit. For the security proof, We used extended mirror theory that systematically estimates the number of solutions to a system of bivariate equations and non-equations. This system of equations and non-equations was converted into a graph theoretic problem. We came up with further detailed calculation, allowing larger components in a graph, compared to DWCDM security proof; to establish the higher security. This improvement ensures that the chances of forgeries against EWCDM or DWCDM is lesser as well requirement of key refreshment shall decrease. However due to nonexistence of any attack, the room for further improvement (say 4n/5 bit) is available yet. This paper co-authored with Dr. Nilanjan Datta and Dr. Avijit Dutta, titled ' Improved Security Bound of (E/D)WCDM', has been accepted in Transactions on Symmetric Cryptology.

Datta, N., Dutta, A., Dutta, K. (2021). Improved Security Bound of (E/D)WCDM. IACR Transactions on Symmetric Cryptology, 2021(4), 138–176.

## 2.2 LightFORK : an alternate construction of LightMAC

In FSE'16, Lyukx et al. proposed two block ciphers based (two independently keyed), a parallel mode PRF 'LightMAC' [3], that achieves a query length independent security of $O(q^2/2^n)$. However the data injection rate was $(n-s)$ bits per primitive invocation(block size n, counter size s) and the maximum length of message was bounded by $(n-s)2^s$ bits. In Asiacrypt'21, Chattopadhyay et al. have shown that LightMAC achieves

the same security even when it is instantiated with a single keyed block cipher [6]. Though the maximum length of message was $(n-s)\ min\{2^{n/4}, 2^s\}$.

On the other hand, in ASIACRYPT '19 a primitive called 'forkcipher'[7] was introduced by Andreeva et al. that outputs two n bit output strings when a s bit tweak and a n bit message is used as input. The output can be visualized as two independent tweakable block cipher outputs. We have proposed an alternative to LightMAC, using this forkcipher. The security bound has been improved from $O(q^2/2^n)$ to $O(q^2/2^{n+s})$. This construction works faster, rate is improved to n bits per primitive invocation. As well the maximum length of message is optimized to $n.2^{n/6+s/2}$ bits. An implementation also showed better performance results in favour of LightFORK. Chattopadhyay et al. came up with the reset-sampling technique[6], in order to avoid unfortunate collisions during primitive outputs that might question the compatibility issue of block cipher. We extended this technique to resetting with delayed sampling for our security proof purpose. We delay while sampling few forkcipher outputs and reset few of them in order to maintain compatibility issue of several forkcipher primitives. This paper titled 'LightFORK: Make LightMAC Faster With FORK' is under review at ToSC.

Along with these mentioned papers, I have read few others such as [8], [9], [10] for my research works.

## 3 Future Research Plans

In the coming days, I want to try to solve more provable security problems of various existing MAC constructions. Also, I want to work with the attack algorithms, that provides tightness of constructions. Moreover my goal is exploring the symmetric cryptography literature in further with application of combinatorics and probability theory.

*The initial progress highlights the opportunities and I am excited to pursue this as a long-term research work in my PhD.*

## References


[1] Benoît Cogliati and Yannick Seurin. Ewcdm: an efficient, beyond-birthday secure, nonce-misuse resistant mac. In *Annual International Cryptology Conference*, pages 121–149. Springer, 2016.

[2] Benoît Cogliati and Yannick Seurin. Analysis of the single-permutation encrypted davies–meyer construction. *Designs, Codes and Cryptography*, 86(12):2703–2723, 2018.

[3] Atul Luykx, Bart Preneel, Elmar Tischhauser, and Kan Yasuda. A mac mode for lightweight block ciphers. In *International Conference on Fast Software Encryption*, pages 43–59. Springer, 2016.

[4] Yu Long Chen, Eran Lambooij, and Bart Mennink. How to build pseudorandom functions from public random permutations. In *Annual International Cryptology Conference*, pages 266–293. Springer, 2019.

[5] Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Kan Yasuda. Encrypt or decrypt? to make a single-key beyond birthday secure nonce-based mac. In *Annual International Cryptology Conference*, pages 631–661. Springer, 2018.

[6] Soumya Chattopadhyay, Ashwin Jha, and Mridul Nandi. Fine-tuning the iso/iec standard lightmac. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 490–519. Springer, 2021.

[7] Elena Andreeva, Virginie Lallemand, Antoon Purnal, Reza Reyhanitabar, Arnab Roy, and Damian Vizár. Forkcipher: a new primitive for authenticated encryption of very short messages. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 153–182. Springer, 2019.

[8] Hwigyeom Kim, Yeongmin Lee, and Jooyoung Lee. Forking tweakable even-mansour ciphers. *IACR Transactions on Symmetric Cryptology*, pages 71–87, 2020.

[9] Benoît Cogliati, Rodolphe Lampe, and Yannick Seurin. Tweaking even-mansour ciphers. In *Annual Cryptology Conference*, pages 189–208. Springer, 2015.

[10] Avijit Dutta, Ashwin Jha, and Mridul Nandi. Tight security analysis of ehtm mac. *IACR Transactions on Symmetric Cryptology*, pages 130–150, 2017.