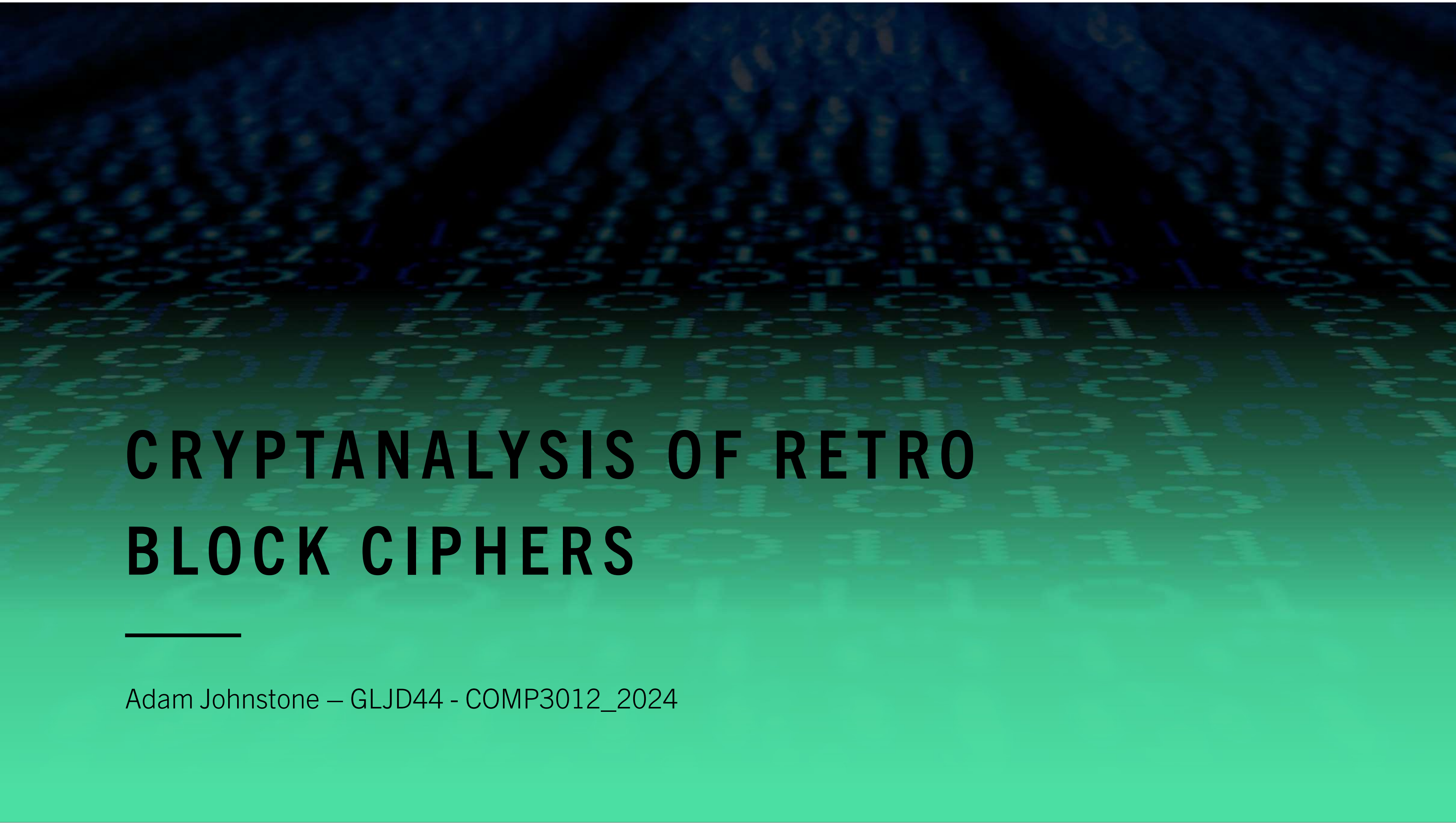


CRYPTANALYSIS OF RETRO BLOCK CIPHERS

Adam Johnstone – GLJD44 - COMP3012_2024

PRESENTATION OUTLINE

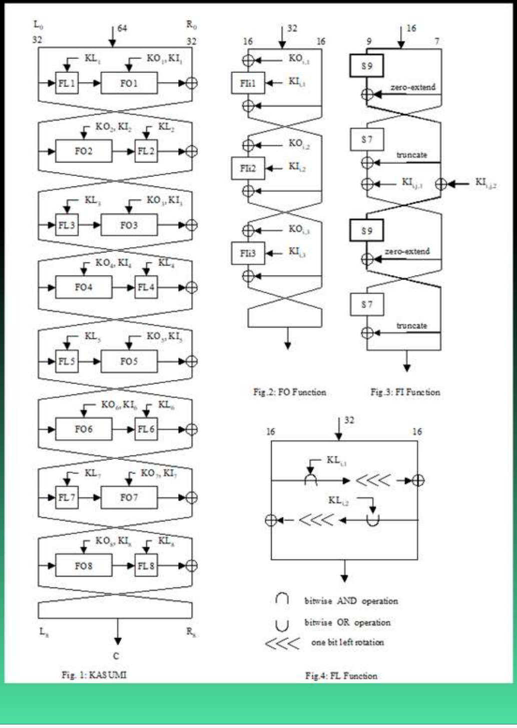
- Background information
- Project Description
- Motivation
- Approach
- Conclusions

BACKGROUND

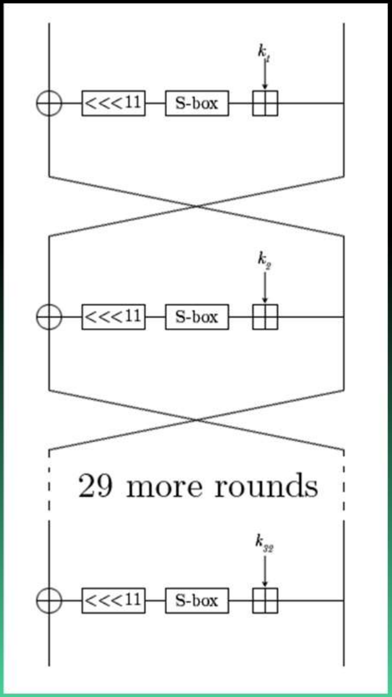
- What is cryptanalysis?
- What is a block cipher?

MY PROJECT

KASUMI



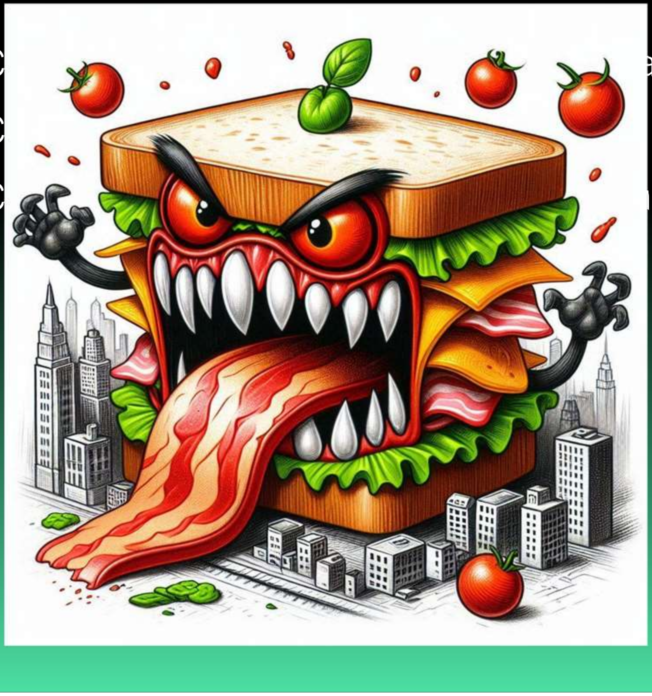
GOST



PROJECT DESCRIPTION

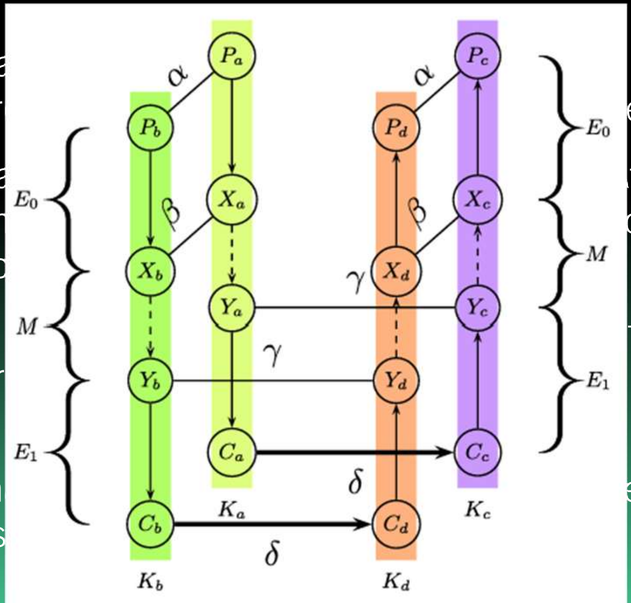
INFORMAL

- C apers
- C
- C to a



FORMAL

- Ca MI and ar e
- Ca ttack on oy ac
- Is for br
- Is project th e used as



A Related-Key Sandwich Quartet

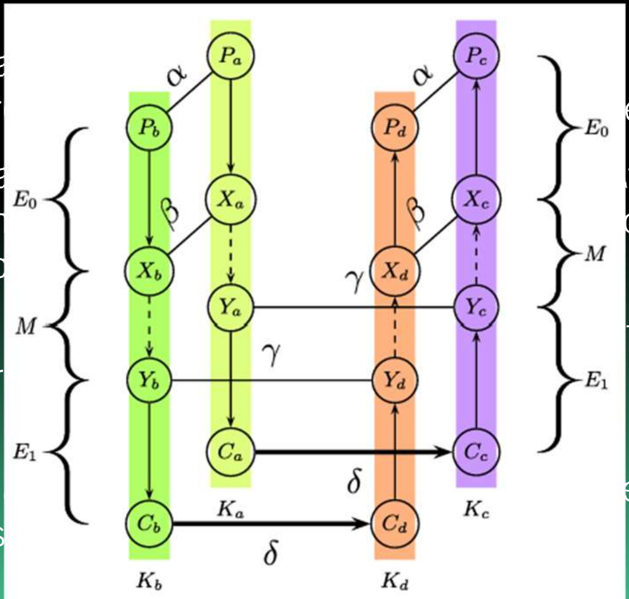
PROJECT DESCRIPTION

INFORMAL

- Can I replicate the findings of published papers
- Can the Sandwich attack break GOST
- Can I draw conclusions about my research to apply to modern cryptanalysis

FORMAL

- Ca MI and ar e
- Ca ttack on by ac
- Is for br
- Is project th e used as



A Related-Key Sandwich Quartet

PROJECT DESCRIPTION

INFORMAL

- Can I replicate the findings of published papers
- Can the Sandwich attack break GOST
- Can I draw conclusions about my research to apply to modern cryptanalysis

FORMAL

- Can I apply the Sandwich attack on KASUMI and are the findings from Shamir et al accurate
- Can I apply the Related Key Boomerang Attack on GOST and are the findings from Rudskoy accurate
- Is the Sandwich attack a feasible method for breaking the GOST block cipher
- Is it possible to draw conclusions from my project that suggest the Sandwich attack could be used as a modern attack method

MOTIVATION

- Sandwich attack created in 2010, hasn’t really been used since despite potentially promising performance improvements
- Due to the Sandwich attack being built upon a Boomerang attack, it could suggest that wherever you can perform a Boomerang attack you can perform a Sandwich attack
- Could lead to an efficient attack on modern block ciphers
- Building upon the limited documentation to aid understanding of the Sandwich attack

MY APPROACH TO THE PROJECT

1. Implement the original Sandwich attack on KASUMI proposed by Shamir et al
2. Implement a Related Key Boomerang Attack on GOST proposed by Rudskoy
3. Perform some analysis on whether an implementation of a Sandwich attack on GOST would be feasible
4. If I think it's feasible then implement a Sandwich attack on GOST
5. If I don’t think it's feasible then add to the Sandwich attack documentation and provide details of my findings e.g. proving why the Sandwich attack doesn’t work on GOST and what would need to change for it to work

CONCLUSIONS

- Can I use the Sandwich attack to break GOST
- Can I break GOST with reasonable constraints
- Does this then have implications for modern block ciphers and cryptanalysis
- Can I improve upon the Sandwich attack literature to help others understand it more easily

BIBLIOGRAPHY

1. Rudskoy, V. (2010). On zero practical significance of “"Key recovery attack on full GOST block cipher with zero time and memory”". Cryptology ePrint Archive, Paper 2010/111. https://eprint.iacr.org/2010/111
2. Dunkelman, O., Keller, N. & Shamir, A. A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony. J Cryptol 27, 824–849 (2014). https://doi.org/10.1007/s00145-013-9154-9
3. Jana, A., Rahman, M., Saha, D., & Paul, G. (2023). Switching the Top Slice of the Sandwich with Extra Filling Yields a Stronger Boomerang for NLFSR-based Block Ciphers. Cryptology ePrint Archive, Paper 2023/1543. https://eprint.iacr.org/2023/1543
4. 3rd Generation Partnership Project, Technical specification group services and system aspects, 3G security. Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification, V18.0.0 (2024)
5. Dolmatov, V., Ed., and D. Baryshkov, "GOST R 34.12-2015: Block Cipher "Magma"", RFC 8891, DOI 10.17487/RFC8891, September 2020, <https://www.rfc-editor.org/info/rfc8891>.