Computability and Complexity in Elliptic Curves and Cryptography

Parity of s-round Generalized AES

Kevin Bombardier
Wichita State University

AAAS Pacific Division Conference

June 24-27, 2012

Collaborators

This is collaborative work with Matthew Cole (University of Notre Dame), Thomas Morrell (Washington University), Cory Scott (Colorado College), and our mentor, Dr. Liljana Babinkostova (Boise State University)

Overview

- Definitions

Overview

- Definitions
- Motivation

Overview

- Definitions
- Motivation
- Results

Overview

- Definitions
- Motivation
- Results
- Conclusions

Overview

- Definitions
- Motivation
- Results
- Conclusions
- Future Work and Recommendations

Definitions

- For any $k \in \mathcal{K}$, we denote the generalized s-round AES permutation $T_s[k] : GF(p^r)^{mn} \rightarrow GF(p^r)^{mn}$ by $T_s[k] = \sigma \circ \pi \circ \lambda \circ (\sigma \circ \rho \circ \pi \circ \lambda)^{s-1} \circ \sigma$.

Definitions

- For any $k \in \mathcal{K}$, we denote the generalized s-round AES permutation $T_s[k] : GF(p^r)^{mn} \rightarrow GF(p^r)^{mn}$ by $T_s[k] = \sigma \circ \pi \circ \lambda \circ (\sigma \circ \rho \circ \pi \circ \lambda)^{s-1} \circ \sigma$.

- For the set of generalized AES permutations we write $\tau_s = \{T_s[k] | k \in \mathcal{K}\}$.

Definitions

- For any $k \in \mathcal{K}$, we denote the generalized s-round AES permutation $T_s[k] : GF(p^r)^{mn} \rightarrow GF(p^r)^{mn}$ by $T_s[k] = \sigma \circ \pi \circ \lambda \circ (\sigma \circ \rho \circ \pi \circ \lambda)^{s-1} \circ \sigma$.
- For the set of generalized AES permutations we write $\tau_s = \{T_s[k] | k \in \mathcal{K}\}$.
- For the group generated by τ_s we write $G_{\tau_s} =< \tau_s >$.

Definitions

- For any $k \in \mathcal{K}$, we denote the generalized s-round AES permutation $T_s[k] : GF(p^r)^{mn} \rightarrow GF(p^r)^{mn}$ by $T_s[k] = \sigma \circ \pi \circ \lambda \circ (\sigma \circ \rho \circ \pi \circ \lambda)^{s-1} \circ \sigma$.
- For the set of generalized AES permutations we write $\tau_s = \{T_s[k] | k \in \mathcal{K}\}$.
- For the group generated by τ_s we write $G_{\tau_s} =< \tau_s >$.
- In particular, we denote "classical" AES as $T_{10}[k] : GF(2^8)^{4\times 4} \rightarrow GF(2^8)^{4\times 4}$ by $T_{10}[k] = \sigma \circ \pi \circ \lambda \circ (\sigma \circ \rho \circ \pi \circ \lambda)^9 \circ \sigma$.

Motivation

- [1]There have already been attacks on classical AES.

[1] Bogdanov, Khovratovich, and Rechberger, *Biclique Cryptanalysis of the Full AES*, 2011.

[2] R. Wernsdorf, *The Round Functions of RIJNDAEL Generate the Alternating Group.*,**Rohde & Schwarz SIT GmbH,, 2002.**

Motivation

- [1]There have already been attacks on classical AES.
- Is there a way to improve the security of AES?

[1] Bogdanov, Khovratovich, and Rechberger, *Biclique Cryptanalysis of the Full AES*, 2011.

[2] R. Wernsdorf, *The Round Functions of RIJNDAEL Generate the Alternating Group.*,**Rohde & Schwarz SIT GmbH,, 2002.**

Motivation

- [1]There have already been attacks on classical AES.
- Is there a way to improve the security of AES?
- Would encrypting multiple times improve the security?

[1] Bogdanov, Khovratovich, and Rechberger, *Biclique Cryptanalysis of the Full AES*, 2011.

[2] R. Wernsdorf, *The Round Functions of RIJNDAEL Generate the Alternating Group.*,**Rohde & Schwarz SIT GmbH,, 2002.**

Motivation

- [1]There have already been attacks on classical AES.
- Is there a way to improve the security of AES?
- Would encrypting multiple times improve the security?
- [2]It is known that τ in classical AES generates $A_{2^{128}}$.

[1] Bogdanov, Khovratovich, and Rechberger, *Biclique Cryptanalysis of the Full AES*, 2011.

[2] R. Wernsdorf, *The Round Functions of RIJNDAEL Generate the Alternating Group.*,**Rohde & Schwarz SIT GmbH,, 2002.**

Motivation

- [1]There have already been attacks on classical AES.
- Is there a way to improve the security of AES?
- Would encrypting multiple times improve the security?
- [2]It is known that τ in classical AES generates $A_{2^{128}}$.
- It is known that τ in classical AES is not a group.

[1] Bogdanov, Khovratovich, and Rechberger, *Biclique Cryptanalysis of the Full AES*, 2011.

[2] R. Wernsdorf, *The Round Functions of RIJNDAEL Generate the Alternating Group.*,**Rohde & Schwarz SIT GmbH,, 2002.**

Motivation

- [1]There have already been attacks on classical AES.
- Is there a way to improve the security of AES?
- Would encrypting multiple times improve the security?
- [2]It is known that τ in classical AES generates $A_{2^{128}}$.
- It is known that τ in classical AES is not a group.
- However, it is unknown what group is generated by τ_s.

[1] Bogdanov, Khovratovich, and Rechberger, *Biclique Cryptanalysis of the Full AES*, 2011.

[2] R. Wernsdorf, *The Round Functions of RIJNDAEL Generate the Alternating Group.*,**Rohde & Schwarz SIT GmbH,, 2002.**

Motivation

- Open Problem: Is AES more secure if a message is encrypted multiple times?

Motivation

- Open Problem: Is AES more secure if a message is encrypted multiple times?
- Open Problem: What group is G_{T_s}? When is it the Alternating Group or the Symmetric Group?

Motivation

- Open Problem: Is AES more secure if a message is encrypted multiple times?
- Open Problem: What group is G_{T_s}? When is it the Alternating Group or the Symmetric Group?
- $T_s[k] = \sigma \circ \pi \circ \lambda \circ (\sigma \circ \rho \circ \pi \circ \lambda)^{s-1} \circ \sigma$

Motivation

- Open Problem: Is AES more secure if a message is encrypted multiple times?
- Open Problem: What group is G_{τ_s}? When is it the Alternating Group or the Symmetric Group?
- $T_s[k] = \sigma \circ \pi \circ \lambda \circ (\sigma \circ \rho \circ \pi \circ \lambda)^{s-1} \circ \sigma$
- When G_{τ_s} is the symmetric group, this is the largest possible group that G_{τ_s} can be.

Motivation

Encrypting multiple times does not improve the security of AES if τ_s is a group. That is, for any keys k_1 and k_2, there exists a key k_3 such that $T_s[k_1] \circ T_s[k_2] = T_s[k_3]$.

Motivation

Encrypting multiple times does not improve the security of AES if τ_s is a group. That is, for any keys k_1 and k_2, there exists a key k_3 such that $T_s[k_1] \circ T_s[k_2] = T_s[k_3]$.

Theorem

Permutation groups contain either all even permutations, or half even and half odd permutations.

Motivation

Encrypting multiple times does not improve the security of AES if τ_s is a group. That is, for any keys k_1 and k_2, there exists a key k_3 such that $T_s[k_1] \circ T_s[k_2] = T_s[k_3]$.

Theorem

Permutation groups contain either all even permutations, or half even and half odd permutations.

We can use this classical theorem to determine whether or not τ_s is a group.

Multiple Rounds

- For $T_s[k]$ to be odd, at least one round function must be both odd and applied an odd number of times.

Multiple Rounds

- For $T_s[k]$ to be odd, at least one round function must be both odd and applied an odd number of times.
- So for λ and π, the number of rounds s must be odd.

Multiple Rounds

- For $T_s[k]$ to be odd, at least one round function must be both odd and applied an odd number of times.
- So for λ and π, the number of rounds s must be odd.
- For ρ, the number of rounds s must be even.

When is AES odd for $p = 2$?

Theorem

When $p = 2$, $T_s[k]$ has odd parity if and only if:

- *m, n, and s are odd; or*
- *$\sum c_i$, s, and r are odd, and n is even.*

When is AES odd for $p = 2$?

Among all possible parities of the variables, we have the following:

When is AES odd for $p = 2$?

Among all possible parities of the variables, we have the following:

When $p = 2$,

- σ and ρ are never odd
- λ is odd in $\frac{1}{8}$ of the cases
- π is odd in $\frac{1}{16}$ of the cases

When is AES odd for $p = 2$?

Among all possible parities of the variables, we have the following:

When $p = 2$,

- σ and ρ are never odd
- λ is odd in $\frac{1}{8}$ of the cases
- π is odd in $\frac{1}{16}$ of the cases
- (These cases do not overlap.)

When is AES odd for $p = 2$?

Among all possible parities of the variables, we have the following:

When $p = 2$,

- σ and ρ are never odd
- λ is odd in $\frac{1}{8}$ of the cases
- π is odd in $\frac{1}{16}$ of the cases
- (These cases do not overlap.)

When $p = 2$, τ_s is a set of odd permutations in $\frac{3}{16}$ of all possible cases.

When is AES odd for $p = 2$?

Among all possible parities of the variables, we have the following:

When $p = 2$,

- σ and ρ are never odd
- λ is odd in $\frac{1}{8}$ of the cases
- π is odd in $\frac{1}{16}$ of the cases
- (These cases do not overlap.)

When $p = 2$, τ_s is a set of odd permutations in $\frac{3}{16}$ of all possible cases.

It follows that τ_s is not a group in these cases.

When is AES odd for p odd?

Theorem

When p is odd, $T_s[k]$ has odd parity if and only if:

- *m, n, and s are odd, $((p^r - 1)/|\langle a \rangle|$ even, and ($p \equiv_4 1$ or r even)); or*
- *m, n, and s are odd, $((p^r - 1)/|\langle a \rangle|$ odd, $p \equiv_4 3$, and r odd); or*
- *$\sum c_i$, r, and s are odd, and n is even; or*
- *$(p^{rm} - 1)/|\langle c \rangle|$ and n are odd, and s is even.*

When is AES odd for p odd?

Among all possible parities of the variables, we have the following:

When is AES odd for p odd?

Among all possible parities of the variables, we have the following:

When p odd,

- σ is never odd
- λ is odd in $\frac{1}{16}$ of the cases
- π is odd in $\frac{1}{16}$ of the cases
- ρ is odd in $\frac{1}{8}$ of the cases

When is AES odd for p odd?

Among all possible parities of the variables, we have the following:

When p odd,

- σ is never odd
- λ is odd in $\frac{1}{16}$ of the cases
- π is odd in $\frac{1}{16}$ of the cases
- ρ is odd in $\frac{1}{8}$ of the cases
- (These cases do not overlap.)

When is AES odd for p odd?

Among all possible parities of the variables, we have the following:

When p odd,

- σ is never odd
- λ is odd in $\frac{1}{16}$ of the cases
- π is odd in $\frac{1}{16}$ of the cases
- ρ is odd in $\frac{1}{8}$ of the cases
- (These cases do not overlap.)

When p odd, τ_s is a set of odd permutations in $\frac{1}{4}$ of all possible cases.

When is AES odd for p odd?

Among all possible parities of the variables, we have the following:

When p odd,

- σ is never odd
- λ is odd in $\frac{1}{16}$ of the cases
- π is odd in $\frac{1}{16}$ of the cases
- ρ is odd in $\frac{1}{8}$ of the cases
- (These cases do not overlap.)

When p odd, τ_s is a set of odd permutations in $\frac{1}{4}$ of all possible cases.

It follows that τ_s is not a group in these cases.

Conclusions

- In the cases when τ_s contains only odd permutations, it cannot be a group.

Conclusions

- In the cases when τ_s contains only odd permutations, it cannot be a group.
- Furthermore, it follows that when τ_s contains only odd permutations, it does not generate $A_{p^{rmn}}$.

Future Work and Recommendations

- Open Problem: So if τ_s does not generate $A_{p^{rmn}}$, does it generate $S_{p^{rmn}}$?

Future Work and Recommendations

- Open Problem: So if τ_s does not generate $A_{p^{rmn}}$, does it generate $S_{p^{rmn}}$?
- Open Problem: When τ_S contains only even permutations, is it a group?

Future Work and Recommendations

- Open Problem: So if τ_s does not generate $A_{p^{rmn}}$, does it generate $S_{p^{rmn}}$?
- Open Problem: When τ_S contains only even permutations, is it a group?
- What if one wishes to keep the number of rounds s even in classical AES, but have τ_S contain only odd permutation?

Future Work and Recommendations

- Open Problem: So if τ_s does not generate $A_{p^{rmn}}$, does it generate $S_{p^{rmn}}$?
- Open Problem: When τ_S contains only even permutations, is it a group?
- What if one wishes to keep the number of rounds s even in classical AES, but have τ_S contain only odd permutation?
- Suggestion: Add a "ShiftBits" permutation in the final round of AES to make every $T_s[k]$ odd.

Future Work and Recommendations

- Open Problem: So if τ_s does not generate $A_{p^{rmn}}$, does it generate $S_{p^{rmn}}$?
- Open Problem: When τ_S contains only even permutations, is it a group?
- What if one wishes to keep the number of rounds s even in classical AES, but have τ_S contain only odd permutation?
- Suggestion: Add a "ShiftBits" permutation in the final round of AES to make every $T_s[k]$ odd.

Future Work and Recommendations

Definition

θ is a *ShiftBits* function if there exists a $c \in \mathbb{Z}_{8mn}$ such that $\theta(x) = y$ if and only if $y_i = x_{i-c \mod 8mn}$ for all $i \in \mathbb{Z}_{8mn}$.

Future Work and Recommendations

Definition

θ is a *ShiftBits* function if there exists a $c \in \mathbb{Z}_{8mn}$ such that $\theta(x) = y$ if and only if $y_i = x_{i-c \mod 8mn}$ for all $i \in \mathbb{Z}_{8mn}$.

So our s-round classical AES permutation becomes $T_s[k] = \theta \circ \sigma \circ \pi \circ \lambda \circ (\sigma \circ \rho \circ \pi \circ \lambda)^{s-1} \circ \sigma$.

Acknowledgements

Thanks to Boise State University and to the National Science Foundation for funding the research under the grant DMS 1062857.