Computability and Complexity in Elliptic Curves and Cryptography

SubBytes, MixColumns, and 1-round AES

Matthew Cole

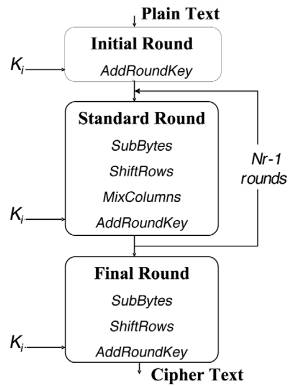
University of Notre Dame

AAAS Pacific Division Conference
June 24-27, 2012

Collaborators

In collaboration with
Dr. Liljana Babinkostova (Boise State University),
Kevin Bombardier (Wichita State University),
Thomas Morrell (Washington University in St. Louis),
and Cory Scott (Colorado College).

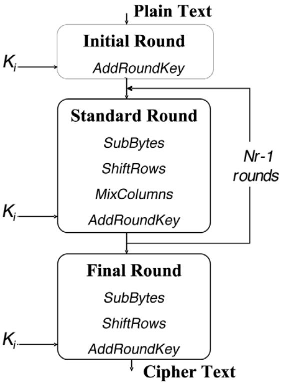
AES Overview



[1]

[1] J. Daemen and V. Rijmen, *AES submission document on Rijndael*, Version 2, (1999)

AES Overview



[1]

My focus: Parity of SubBytes and MixColumns, followed by 1-round AES-like functions.

[1] J. Daemen and V. Rijmen, *AES submission document on Rijndael*, Version 2, (1999)

SubBytes

Recall that the plaintext can be represented as a matrix.

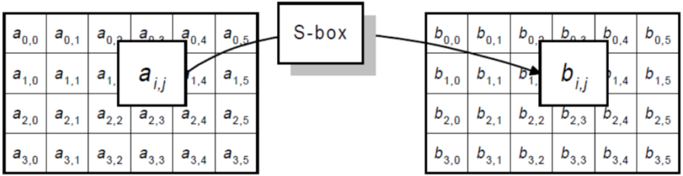
[2] J. Daemen and V. Rijmen, *AES submission document on Rijndael*, Version 2, (1999)

SubBytes

Recall that the plaintext can be represented as a matrix.

Definition

The function $\lambda : M_{m,n}((GF(p^r)) \rightarrow M_{m,n}((GF(p^r))$ is called a *SubBytes function* if it is the parallel application of mn bijective S-box-mappings $\lambda_{ij} : GF(p^r) \rightarrow GF(p^r)$ defined by $\lambda(a) = b$ if and only if $b_{ij} = \lambda_{ij}(a_{ij})$ for all $0 \leq i < m, 0 \leq j < n$.

[2] 

[2] J. Daemen and V. Rijmen, *AES submission document on Rijndael*, Version 2, (1999)

SubBytes

SubBytes puts each element in the matrix through an 'S-box' λ_{ij} given by

$$\lambda_{ij}(x) = ax^{-1} + b$$

where

- a is a degree $r - 1$ polynomial
- x^{-1} is the inverse of the element over $GF(p^r)$
- b is a fixed element of $GF(p^r)$.

SubBytes

SubBytes puts each element in the matrix through an 'S-box' λ_{ij} given by

$$\lambda_{ij}(x) = ax^{-1} + b$$

where

- a is a degree $r - 1$ polynomial
- x^{-1} is the inverse of the element over $GF(p^r)$
- b is a fixed element of $GF(p^r)$.

The S-box is usually implemented as a lookup table.

SubBytes

Lemma

Let a be the fixed polynomial by which x^{-1} is multiplied in the S-box. The SubBytes function λ is an odd permutation iff:

SubBytes

Lemma

Let a be the fixed polynomial by which x^{-1} is multiplied in the S-box. The SubBytes function λ is an odd permutation iff:

- m and n are both odd, and
- Each individual S-box λ_{ij} is odd:

SubBytes

Lemma

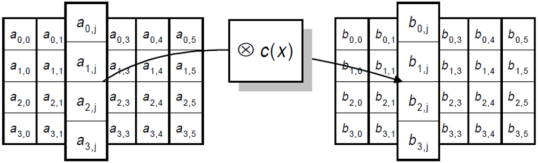
Let a be the fixed polynomial by which x^{-1} is multiplied in the S-box. The SubBytes function λ is an odd permutation iff:

- m and n are both odd, and
- Each individual S-box λ_{ij} is odd:
  - $p \equiv_4 3$, r is odd, and $(p^r - 1)/\left|\langle a \rangle\right|$ is odd, OR
  - either $p \equiv_4 1$ or r is even, and $(p^r - 1)/\left|\langle a \rangle\right|$ is even, OR
  - $p = 2$ and $r > 1$.

MixColumns

Definition

ρ is a *MixColumns function* if it is an invertible linear transformation over $M_{m,n}(GF(p^r))$, ie, there is an invertible matrix $D \in M_{m,m}(GF(p^r))$ such that
$\rho(x) = Dx, \quad \forall x \in M_{m,n}(GF(p^r))$.



[3]

[3] J. Daemen and V. Rijmen, *AES submission document on Rijndael*, Version 2, (1999)

MixColumns

- The MixColumns function multiplies each column of the state by an invertible matrix.

MixColumns

- The MixColumns function multiplies each column of the state by an invertible matrix.
- Alternatively, this function can be represented as multiplication by a fixed polynomial over $GF(p^r)$, mod another fixed polynomial of degree m coprime to that one.

MixColumns

- The MixColumns function multiplies each column of the state by an invertible matrix.
- Alternatively, this function can be represented as multiplication by a fixed polynomial over $GF(p^r)$, mod another fixed polynomial of degree m coprime to that one.
- In classical AES, this polynomial is $c(x) = \texttt{0x03}x^3 + \texttt{0x01}x^2 + \texttt{0x01}x + \texttt{0x02}$, and the modulus is $p(x) = x^4 + 1$.

MixColumns

- The MixColumns function multiplies each column of the state by an invertible matrix.
- Alternatively, this function can be represented as multiplication by a fixed polynomial over $GF(p^r)$, mod another fixed polynomial of degree m coprime to that one.
- In classical AES, this polynomial is $c(x) = \mathtt{0x03}x^3 + \mathtt{0x01}x^2 + \mathtt{0x01}x + \mathtt{0x02}$, and the modulus is $p(x) = x^4 + 1$.

Lemma

The MixColumns function ρ is an odd permutation if and only if p and n are both odd, and $(p^{rm} - 1)/\left|\langle c \rangle\right|$ is odd, where c is the fixed polynomial of the MixColumns function ρ.

1-round AES Functions

1-round AES Functions

Definition

For any $k \in \mathcal{K}$, a *generalized 1-round AES permutation* $T[k] : GF(p^r)^{mn} \to GF(p^r)^{mn}$ is a permutation of the form $T[k] = \sigma[k] \circ \rho \circ \pi \circ \lambda$ where

λ	is a SubBytes function,
π	is a ShiftRows function,
ρ	is a MixColumns function, and
$\sigma[k]$	is the AddRoundKey function with key k.

1-round AES Functions

Definition

For any $k \in \mathcal{K}$, a *generalized 1-round AES permutation* $T[k] : GF(p^r)^{mn} \to GF(p^r)^{mn}$ is a permutation of the form $T[k] = \sigma[k] \circ \rho \circ \pi \circ \lambda$ where

λ	is a SubBytes function,
π	is a ShiftRows function,
ρ	is a MixColumns function, and
$\sigma[k]$	is the AddRoundKey function with key k.

- For the set of 1-round AES functions we write $\tau := \{T[k] | k \in \mathcal{K}\}$.

1-round AES Functions

Definition

For any $k \in \mathcal{K}$, a *generalized 1-round AES permutation* $T[k] : GF(p^r)^{mn} \to GF(p^r)^{mn}$ is a permutation of the form $T[k] = \sigma[k] \circ \rho \circ \pi \circ \lambda$ where

λ	is a SubBytes function,
π	is a ShiftRows function,
ρ	is a MixColumns function, and
$\sigma[k]$	is the AddRoundKey function with key k.

- For the set of 1-round AES functions we write $\tau := \{T[k] | k \in \mathcal{K}\}$.
- For the group generated by τ we write $G_\tau := \langle \tau \rangle$.

1-round AES Functions

Theorem

One-round classical AES generates the alternating group.[a]

[a] R. Wernsdorf, *The Round Functions of RIJNDAEL Generate the Alternating Group*, 2002

1-round AES Functions

Theorem

One-round classical AES generates the alternating group.[a]

[a] R. Wernsdorf, *The Round Functions of RIJNDAEL Generate the Alternating Group*, 2002

Corollary

One-round classical AES is not a group.

1-round AES Functions

Theorem

One-round classical AES generates the alternating group.[a]

[a] R. Wernsdorf, *The Round Functions of RIJNDAEL Generate the Alternating Group*, 2002

Corollary

One-round classical AES is not a group.

Open problem: what group do general 1-round AES permutations generate?

1-round AES Functions

Theorem

One-round classical AES generates the alternating group.[a]

[a] R. Wernsdorf, *The Round Functions of RIJNDAEL Generate the Alternating Group*, 2002

Corollary

One-round classical AES is not a group.

Open problem: what group do general 1-round AES permutations generate?

We suspect it is always the alternating or symmetric group.

Tools: Transitivity

Let G be a permutation group over a set X.

Definition

G is *transitive* if $\forall(a, b)$, a, $b \in X$, $\exists\sigma \in G$ such that $\sigma(a) = b$.

Tools: Transitivity

Let G be a permutation group over a set X.

Definition

G is *transitive* if $\forall(a, b)$, a, $b \in X$, $\exists\sigma \in G$ such that $\sigma(a) = b$.

Lemma

The group generated by 1-round AES functions over $M_{m,n}(GF(2^r))$ is transitive $\forall m, n, r$.[a]

[a] R. Sparr and R. Wernsdorf, *Group Theoretic Properties of Rijndael-like ciphers*, 2008

Tools: Transitivity

Let G be a permutation group over a set X.

Definition

G is *transitive* if $\forall(a, b)$, a, $b \in X$, $\exists\sigma \in G$ such that $\sigma(a) = b$.

Lemma

The group generated by 1-round AES functions over $M_{m,n}(GF(2^r))$ is transitive $\forall m, n, r$.[a]

[a] R. Sparr and R. Wernsdorf, *Group Theoretic Properties of Rijndael-like ciphers*, 2008

Lemma

The group generated by 1-round AES functions over $M_{m,n}(GF(p^r))$ is transitive $\forall p, m, n, r$.

Current Work: ℓ-Transitivity

Let G be a permutation group over a set X.

Can we use existing theorems to answer our conjecture?

Current Work: ℓ-Transitivity

Let G be a permutation group over a set X.

Can we use existing theorems to answer our conjecture?

Definition

G is *ℓ-transitive* if $\forall (a_i, b_i)$, a_i, $b_i \in X$, $1 \leq i \leq \ell$, such that $a_j \neq a_k$ and $b_j \neq b_k$ when $j \neq k$, $\exists \sigma \in G$ such that $\sigma(a_i) = b_i$.

Current Work: ℓ-Transitivity

Let G be a permutation group over a set X.

Can we use existing theorems to answer our conjecture?

Definition

G is *ℓ-transitive* if $\forall (a_i, b_i)$, a_i, $b_i \in X$, $1 \leq i \leq \ell$, such that $a_j \neq a_k$ and $b_j \neq b_k$ when $j \neq k$, $\exists \sigma \in G$ such that $\sigma(a_i) = b_i$.

Theorem

If G is a 2-transitive group of degree N containing a p-cycle where p is prime and $N/2 < p \leq N - 3$, then G is the alternating or symmetric group. [a]

[a] D. M. Rodgers, *Generating and covering the alternating of symmetric group*, Communications in Algebra, 2002

Current Work: Primitivity

Let G be a permutation group over a set X.

Can we use existing theorems to answer our conjecture?

Current Work: Primitivity

Let G be a permutation group over a set X.

Can we use existing theorems to answer our conjecture?

Definition

A set $B = \{b_1, \ldots, b_k\} \subset X$ is a *block* under G if $\forall \sigma \in G$, either $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$.

Definition

G is *primitive* if $\nexists$ any nontrivial block of X under G.

Current Work: Primitivity

Let G be a permutation group over a set X.

Can we use existing theorems to answer our conjecture?

Definition

G is *primitive* if $\nexists$ any nontrivial block of X under G.

Current Work: Primitivity

Let G be a permutation group over a set X.

Can we use existing theorems to answer our conjecture?

Definition

G is *primitive* if $\nexists$ any nontrivial block of X under G.

Theorem

If G is a primitive group of degree N containing an M-cycle where $2 \leq M \leq (N-M)!$, then G is the alternating or symmetric group. [a]

[a] D. M. Rodgers, *Generating and covering the alternating of symmetric group*, Communications in Algebra, 2002

Acknowledgements

Thanks to Boise State University and the organizers of its 2012 Mathematics REU for hosting and encouraging our research,

and the National Science Foundation for funding it under grant DMS 1062857.