DES over Finite Groups

L. Babinkostova[1], A. Bowden[2], A. Kimball[3], and K. Williams[1]

[1]Boise State University, [2]Loyola Marymount University, [3]Western Carolina University

July 29, 2011

1. Introduction
2. How the Project Progressed
3. Main Results
   - DES over Finite Groups
   - Simplified Version of DES over an Elliptic Curve Group
4. Future Work

What is Data Encryption?

- Process of scrambling data so that it can be decoded only by the intended recipient.
- Uses a mathematical algorithm with a key to encode a file into a form that cannot be read.
- Used to protect government records, military secrets and majority of businesses.

DES: The First Encryption Standard

- Symmetric block data encryption technique.
- Published by the National Bureau of Standards in 1975.
- Accepted as a federal encryption standard in the U.S. in 1977, and later internationally.

Symmetric and Asymmetric Encryption

Symmetric Encryption requires that both the sender and the receiver share the same key and also keep it secret from anyone else.

Symmetric and Asymmetric Encryption

Symmetric Encryption requires that both the sender and the receiver share the same key and also keep it secret from anyone else.

Asymmetric encryption uses two keys, one public and one private. The public key is used to encrypt a message, and the private key is used to decrypt it.

Use of the Data Encryption Standard

- Electronic financial transactions
- Secure data communications
- Protection of passwords or PINs against unauthorized access.

"Whoever you are, I can guarantee that many times in your life, the security of your data was protected by DES."

Bruce Schneier, 2004

Overview of DES

- Keyspace: $\mathcal{K} = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (56 copies of $\mathbb{Z}_2$).
- $|\mathcal{K}| = 2^{56}$.

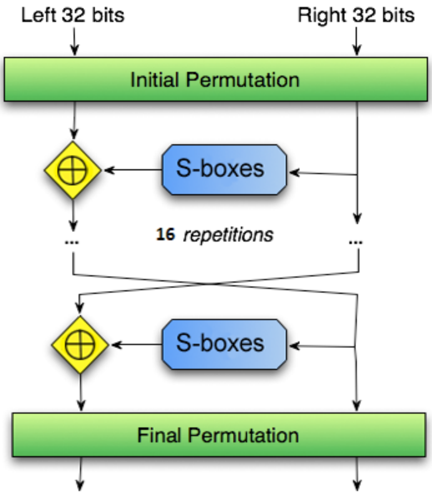
Overview of DES

- Keyspace: $\mathcal{K} = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (56 copies of $\mathbb{Z}_2$).
- $|\mathcal{K}| = 2^{56}$.
- Plaintext space: $\mathcal{P} = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (64 copies of $\mathbb{Z}_2$).
- Ciphertext space: $\mathcal{C} = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (64 copies of $\mathbb{Z}_2$)
- $|\mathcal{P}| = |\mathcal{C}| = 2^{64}$.

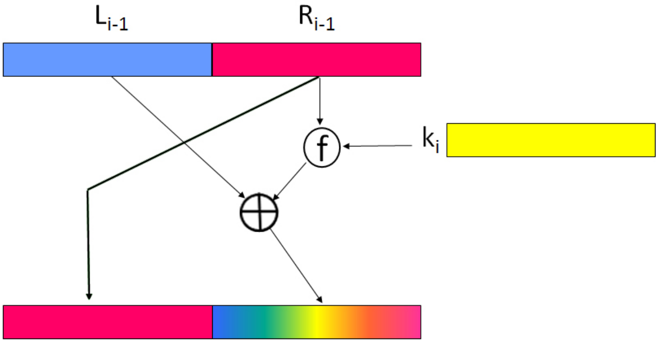
Overview of DES

- Keyspace: $\mathcal{K} = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (56 copies of $\mathbb{Z}_2$).
- $|\mathcal{K}| = 2^{56}$.
- Plaintext space: $\mathcal{P} = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (64 copies of $\mathbb{Z}_2$).
- Ciphertext space: $\mathcal{C} = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (64 copies of $\mathbb{Z}_2$)
- $|\mathcal{P}| = |\mathcal{C}| = 2^{64}$.
- For each key $K \in \mathcal{K}$, the encryption function $e_K : \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 \to \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ has a very technical, but clear, description.
- Each $e_K \in \mathcal{E}$ is a permutation of the set $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (64 copies of $\mathbb{Z}_2$).
- Each decryption $d_K \in \mathcal{D}$ is a permutation of the set $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (64 copies of $\mathbb{Z}_2$).
- $|\mathcal{E}| = |\mathcal{D}| = 2^{56}$.

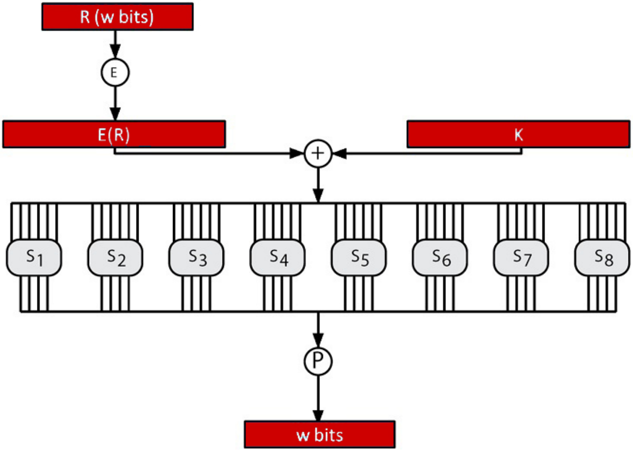
Outline of DES



Feistel Round



Feistel Function



The Security of DES

In 1988, Kaliski, R. Rivest and A. Sherman asked several important questions relevant to the security of DES: [1]

[1] Is the data encryption standard a group?, J. Cryptology (1988) 1: 3-36

The Security of DES

In 1988, Kaliski, R. Rivest and A. Sherman asked several important questions relevant to the security of DES: [1]

Question 1: Is DES a group?

[1] Is the data encryption standard a group?, J. Cryptology (1988) 1: 3-36

The Security of DES

In 1988, Kaliski, R. Rivest and A. Sherman asked several important questions relevant to the security of DES: [1]

Question 1: Is DES a group?

Question 2: What is the group that is generated by DES?

[1] Is the data encryption standard a group?, J. Cryptology (1988) 1: 3-36

The Security of DES

In 1988, Kaliski, R. Rivest and A. Sherman asked several important questions relevant to the security of DES: [1]

Question 1: Is DES a group?

Question 2: What is the group that is generated by DES?

Question 3: Is DES pure?

[1] Is the data encryption standard a group?, J. Cryptology (1988) 1: 3-36

The Security of DES

In 1988, Kaliski, R. Rivest and A. Sherman asked several important questions relevant to the security of DES: [1]

Question 1: Is DES a group?

Question 2: What is the group that is generated by DES?

Question 3: Is DES pure?

Question 4: Is DES faithful?

[1] Is the data encryption standard a group?, J. Cryptology (1988) 1: 3-36

The Security of DES

In 1988, Kaliski, R. Rivest and A. Sherman asked several important questions relevant to the security of DES: [1]

Question 1: Is DES a group?

Question 2: What is the group that is generated by DES?

Question 3: Is DES pure?

Question 4: Is DES faithful?

There is either a conclusive proof or statistical evidence that gives an answer to all these questions for DES over $\mathbb{Z}_2$ only.

[1] Is the data encryption standard a group?, J. Cryptology (1988) 1: 3-36

Initial Work

- We studied two simplified version of DES:
  - B-DES encrypts over $\mathbb{Z}_2$. It uses six Feistel rounds, a 12-bit message, and a 9-bit key.[2]
  - S-DES encrypts over $\mathbb{Z}_2$. It uses two Feistel rounds, an 8-bit message, and a 10-bit key.[3]

[2] W. Trappe, L. Washington, *Introduction to Cryptography*, 2006

[3] E. F. Schaefer, *S-DES algorithm*, Cryptologia, 1996

Initial Work

- We studied two simplified version of DES:
  - B-DES encrypts over $\mathbb{Z}_2$. It uses six Feistel rounds, a 12-bit message, and a 9-bit key.[2]
  - S-DES encrypts over $\mathbb{Z}_2$. It uses two Feistel rounds, an 8-bit message, and a 10-bit key.[3]
- We created a program in Maple to analyze S-DES over the groups $U(5)$ and $U(8)$. Then, using a combination of Coppersmith method and known algebraic results, we proved the following:

[2] W. Trappe, L. Washington, *Introduction to Cryptography*, 2006

[3] E. F. Schaefer, *S-DES algorithm*, Cryptologia, 1996

Initial Work

- We studied two simplified version of DES:
  - B-DES encrypts over $\mathbb{Z}_2$. It uses six Feistel rounds, a 12-bit message, and a 9-bit key.[2]
  - S-DES encrypts over $\mathbb{Z}_2$. It uses two Feistel rounds, an 8-bit message, and a 10-bit key.[3]
- We created a program in Maple to analyze S-DES over the groups $U(5)$ and $U(8)$. Then, using a combination of Coppersmith method and known algebraic results, we proved the following:

Theorem

B-DES and S-DES over U(5) and U(8) are not groups.

[2] W. Trappe, L. Washington, *Introduction to Cryptography*, 2006

[3] E. F. Schaefer, *S-DES algorithm*, Cryptologia, 1996

More Results

We extended our existing Maple software and proved the following:

Theorem

S-DES does not form a group over $\mathbb{Z}_n$ (for certain S-boxes) when n is divisible by 2, 3, 5, 7, or 11.

Theorem

Let G be a finite group. Then S-DES does not form a group over $\mathbb{Z}_n \times G$ (for certain S-boxes) when n is divisible by 2, 3, 5, 7, or 11.

DES-Like Functions

Definition

Suppose that G is a group and $k > 1$. A **DES-like function** on G^{2k} is a transformation δ_f on G^{2k} determined by a function $f : G^k \to G^k$ as follows:

DES-Like Functions

Definition

Suppose that G is a group and $k > 1$. A **DES-like function** on G^{2k} is a transformation δ_f on G^{2k} determined by a function $f : G^k \to G^k$ as follows:

$$\delta_f(\bar{x}, \bar{y}) = (\bar{y}, \bar{x} \oplus f(\bar{y})),$$

where $\bar{x}, \bar{y} \in G^k$ and $\oplus$ is the group operation of G.

DES-Like Functions

Definition

Suppose that G is a group and $k > 1$. A **DES-like function** on G^{2k} is a transformation δ_f on G^{2k} determined by a function $f : G^k \to G^k$ as follows:

$$\delta_f(\bar{x}, \bar{y}) = (\bar{y}, \bar{x} \oplus f(\bar{y})),$$

where $\bar{x}, \bar{y} \in G^k$ and $\oplus$ is the group operation of G.

Theorem

The set of all δ_f (on fixed G^{2k}) does not form a group under composition.

S-DES

Definition

S-DES is a function $S_k = \theta \circ \delta_{f_2} \circ \delta_{f_1}$, where θ is a right-left swap and δ_{f_1} and δ_{f_2} are the functions corresponding to the first and second key schedule (for some fixed S-box).

S-DES

Definition

S-DES is a function $S_k = \theta \circ \delta_{f_2} \circ \delta_{f_1}$, where θ is a right-left swap and δ_{f_1} and δ_{f_2} are the functions corresponding to the first and second key schedule (for some fixed S-box).

We can rewrite this using the definition of δ_{f_i}:

$$S(\bar{x}, \bar{y}) = (\bar{y} \oplus f_2(\bar{x} \oplus f_1(\bar{y})), \bar{x} \oplus f_1(\bar{y})).$$

S-DES with Constant S-boxes

Theorem

Let G be a finite group. Consider a version of S-DES over G for which each entry in every S-box is some fixed element $g \in G$. Then the following are true:

S-DES with Constant S-boxes

Theorem

Let G be a finite group. Consider a version of S-DES over G for which each entry in every S-box is some fixed element $g \in G$. Then the following are true:

1. *S-DES (over all possible keys) does not form a group under functional composition.*

S-DES with Constant S-boxes

Theorem

Let G be a finite group. Consider a version of S-DES over G for which each entry in every S-box is some fixed element $g \in G$. Then the following are true:

1. *S-DES (over all possible keys) does not form a group under functional composition.*
2. *The group generated by S-DES is a cyclic group of order* $\mathrm{lcm}(2, |g|)$.

S-DES is Not a Group

Theorem

S-DES over a group of order ≥ 2 is not a group for any S-box.

DES-Like Encryptions

Definition

A **DES-like encryption** with m rounds is a function $D = \theta \circ \delta_m \circ \ldots \circ \delta_2 \circ \delta_1$, where $\delta_{f_i}(\bar{x}, \bar{y}) = (\bar{y}, \bar{x} \oplus f_i(\bar{y}))$ and $\theta(\bar{x}, \bar{y}) = (\bar{y}, \bar{x})$.

DES-Like Encryptions with Constant S-boxes

Theorem

Let D_k be a family of DES-like encryptions with $m \geq 2$ rounds, different keys, and constant S-boxes that return $g \in G$. If m is even or $|g| > 2$, then the following are true:

DES-Like Encryptions with Constant S-boxes

Theorem

Let D_k be a family of DES-like encryptions with $m \geq 2$ rounds, different keys, and constant S-boxes that return $g \in G$. If m is even or $|g| > 2$, then the following are true:

1. *The set of such encryptions does not form a group under composition.*

DES-Like Encryptions with Constant S-boxes

Theorem

Let D_k be a family of DES-like encryptions with $m \geq 2$ rounds, different keys, and constant S-boxes that return $g \in G$. If m is even or $|g| > 2$, then the following are true:

1. *The set of such encryptions does not form a group under composition.*
2. *The group generated by these encryptions is a cyclic group of order $|g|$ if m is odd, or $\operatorname{lcm}(2, |g|)$ if m is even.*

DES-Like Encryptions with Constant S-boxes

Theorem

Let D_k be a family of DES-like encryptions with $m \geq 2$ rounds, different keys, and constant S-boxes that return $g \in G$. If m is even or $|g| > 2$, then the following are true:

1. *The set of such encryptions does not form a group under composition.*
2. *The group generated by these encryptions is a cyclic group of order $|g|$ if m is odd, or $\mathrm{lcm}(2, |g|)$ if m is even.*

Theorem

A DES-like encryption over a finite group with constant S-boxes is not faithful.

DES is Not a Group

Theorem

A DES-like encryption over a finite group of order ≥ 2 does not form a group unless both of the following hold:

1. *The DES-like encryption has an odd number of Feistel rounds.*
2. *Every element of every S-box is the identity.*

Groups Generated by DES-Like Encryptions

In 1983 S. Even and O. Goldreich showed that DES-Like functions over $\mathbb{Z}_2$ can generate the alternating group.[4]

[4] S. Even and O. Goldreich, *DES-Like Functions Can Generate the Alternating Group*, **IEEE Transactions on Information Theory 29(6)**, 863-865 (1983)

Groups Generated by DES-Like Encryptions

In 1983 S. Even and O. Goldreich showed that DES-Like functions over $\mathbb{Z}_2$ can generate the alternating group.[4]

Theorem

Let G be a group such that $|G|$ is odd and $|G|^k \bmod 4 \equiv 3$, where k is an odd integer. Then the group of permutations generated by the DES-like function $\delta_f : G^{2k} \to G^{2k}$ contains odd permutations.

[4] S. Even and O. Goldreich, *DES-Like Functions Can Generate the Alternating Group*, **IEEE Transactions on Information Theory 29(6)**, 863-865 (1983)

Groups Generated by DES-Like Encryptions

In 1983 S. Even and O. Goldreich showed that DES-Like functions over $\mathbb{Z}_2$ can generate the alternating group.[4]

Theorem

Let G be a group such that $|G|$ is odd and $|G|^k \bmod 4 \equiv 3$, where k is an odd integer. Then the group of permutations generated by the DES-like function $\delta_f : G^{2k} \to G^{2k}$ contains odd permutations.

Corollary

Let G be a group such that $|G|$ is odd and $|G|^k \bmod 4 \equiv 3$, where k is an odd integer. Then the group of permutations generated by the DES-like function $\delta_f : G^{2k} \to G^{2k}$ is either $S_{|G|^{2k}}$ or a subgroup H of $S_{|G|^{2k}}$ such that half of the elements in H are even permutations.

[4] S. Even and O. Goldreich, *DES-Like Functions Can Generate the Alternating Group*, **IEEE Transactions on Information Theory 29(6)**, 863-865 (1983)

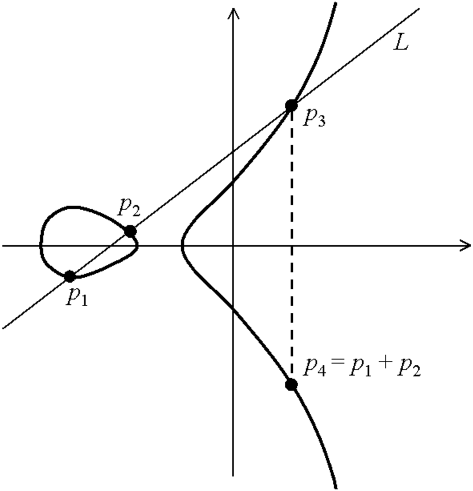
Elliptic Curves

An **Elliptic Curve** is given by an equation of the form

$$y^2 = x^3 + Ax + B,$$

where A and B are constants and the discriminant $\Delta = 4A^3 + 27B^2$ is nonzero.

Addition on an Elliptic Curve



Addition on an Elliptic Curve

Theorem

The addition of points on $E = \{(x, y) : y^2 = x^3 + Ax + B\} \cup \{\infty\}$ *satisfies the following properties:*

1. *Commutativity:* $P_1 + P_2 = P_2 + P_1$ *for all* P_1, P_2 *on* E.
2. *Existence of Identity:* $P + \infty = P$ *for all points* P *on* E.
3. *Existence of Inverses: Given a point* P *on* E, *there exists a point* P' *on* E *such that* $P + P' = \infty$.
4. *Associativity:* $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ *for all* P_1, P_2, P_3 *on* E.

Addition on an Elliptic Curve

Theorem

The addition of points on $E = \{(x, y) : y^2 = x^3 + Ax + B\} \cup \{\infty\}$ *satisfies the following properties:*

1. *Commutativity:* $P_1 + P_2 = P_2 + P_1$ *for all* P_1, P_2 *on* E.
2. *Existence of Identity:* $P + \infty = P$ *for all points* P *on* E.
3. *Existence of Inverses: Given a point* P *on* E, *there exists a point* P' *on* E *such that* $P + P' = \infty$.
4. *Associativity:* $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ *for all* P_1, P_2, P_3 *on* E.

In other words, the points on E *form an additive abelian group with* ∞ *as the identity element.*

Elliptic Curves Over Finite Fields

Theorem

Let E be an elliptic curve over a finite field. Then $E \cong \mathbb{Z}_n$ or $E \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ for some integers $n_1, n_2 \geq 1$ such that $n_1 | n_2$.

Elliptic Curves Over Finite Fields

Theorem

Let E be an elliptic curve over a finite field. Then $E \cong \mathbb{Z}_n$ or $E \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ for some integers $n_1, n_2 \geq 1$ such that $n_1 | n_2$.

Theorem

Let E be an elliptic curve over a finite field. If DES is not a group over $\mathbb{Z}_n$ for any n, then there exist S-boxes such that DES is not a group over the finite field.

E-DES

We developed a simplified version of DES so that we would have an encryption system that is not a group and does not generate the alternating group.

E-DES

We developed a simplified version of DES so that we would have an encryption system that is not a group and does not generate the alternating group.

Theorem

Let G be a group with odd order such that $|G|^k \mod 4 \equiv 3$. Then the group of permutations generated by the DES-like functions $\delta_f : G^{2k} \to G^{2k}$ contains odd permutations.

E-DES

- Encrypts over the elliptic curve $y^2 \equiv x^3 + 4 \mod 7$

E-DES

- Encrypts over the elliptic curve $y^2 \equiv x^3 + 4 \mod 7$
- Message length: 10 bits
- Key length: 12 bits
- Expander function: $[r_5 r_1 r_2 r_3 r_4 r_2 r_3 r_4 r_5 r_1]$
- Key schedule: $K_1 = [k_2 k_{10} k_8 k_9 k_1 k_5 k_{11} k_7 k_6 k_5]$ and $K_2 = [k_2 k_3 k_1 k_6 k_{10} k_9 k_5 k_{11} k_{12} k_4]$

E-DES

- Encrypts over the elliptic curve $y^2 \equiv x^3 + 4 \mod 7$
- Message length: 10 bits
- Key length: 12 bits
- Expander function: $[r_5 r_1 r_2 r_3 r_4 r_2 r_3 r_4 r_5 r_1]$
- Key schedule: $K_1 = [k_2 k_{10} k_8 k_9 k_1 k_5 k_{11} k_7 k_6 k_5]$ and $K_2 = [k_2 k_3 k_1 k_6 k_{10} k_9 k_5 k_{11} k_{12} k_4]$
- Two S-boxes are 9×9 with 2-nit outputs. Each row and column is a permutation of the elements of $\mathbb{Z}_3 \times \mathbb{Z}_3$.
- One S-box is 3×3 with a 1-nit output. Each row and column is a permutation of the elements of $\mathbb{Z}_3$.

Future Work

Solve the following open problems related to the security of DES over finite groups:

- What is the order of the group generated by DES?
- Is DES pure?
- Is DES faithful?

Future Work

Solve the following open problems related to the security of DES over finite groups:

- What is the order of the group generated by DES?
- Is DES pure?
- Is DES faithful?

Improve the security of E-DES in the following ways:

- Construct S-boxes that satisfy specific properties.
- Design a new key schedule using the Discrete Log Problem.

References

- Nicolas T. Courtois, Guilhem Castagnos, and Louis Goubin, *What Do DES S-boxes Say to Each Other?*, **Cryptographic Research & Advanced Security** (2003).
- Shimon Even and Oded Goldreich, *DES-Like Functions Can Generate the Alternating Group*, **IEEE Transactions on Information Theory 29(6)**, 863-865 (1983).
- W. Trappe, L. Washington, *Introduction to Cryptography*, (2006).
- E. F. Schaefer, *S-DES algorithm*, Cryptologia, (1996).
- S. Even and O. Goldreich, *DES-Like Functions Can Generate the Alternating Group*, **IEEE Transactions on Information Theory 29(6)**, 863-865 (1983).
- L. Washington, *Elliptic Curve Cryptography*, (2009).
- B. Kaliski et al. *Is the data encryption standard a group?*, **J. Cryptology**, 3-36 (1988).
- K. Campbell and M. Wiener, *DES is not a Group*, **CRYPTO '92**.
- R. Wernsdorf, *The One-Round Functions of the DES Generate the Alternating Group*, **EUROCRYPT '92**.
- D. Copersmith and E. Grossman, *generators of Certain Alternating Groups with Applications to Cryptography*, **SIAM Journal on Applied mathematics**, Vol. 29, No. 4, 624-627 (1975).
- L. Miller, *Generators of the Symmetric and Alternating Groups*, **The American Mathematical Monthly**, Vol. 48, No.1, 43-44 (1942).