Symmetric key cryptography over non-binary algebraic structures

Kameryn J Williams

Boise State University

26 June 2012
AAAS Pacific Conference 24-27 June 2012

Acknowledgments

These results are due to collaboration with Liljana Babinkostova, Alyssa Bowden, and Andrew Kimball starting at the 2011 Boise State University REU in Mathematics.
We gratefully acknowledge NSF grant DMS 1062857 and Boise State University for their support.

Algebraic security properties of DES

Problem (1988 Kaliski, Rivest, and Sherman[1])

- *Does the set of DES encryptions form a group?*
- *What is the group generated by DES?*
- *Is DES* pure*? For all keys j, k, ℓ is there a key m such that $E_j \circ E_k^{-1} \circ E_\ell = E_m$?*

[1] B. S. Kaliski, R. L. Rivest, and A. T. Sherman, "Is the Data Encryption Standard a group?", *J. Cryptology* (1988).

Algebraic security properties of DES

Theorem (1992 Campbell and Wiener[2])

DES does not form a group.

[2] K. W. Campbell and M. J. Wiener, "DES is not a group", *Advances in Cryptology—CRYPTO '92, LNCS* (2003).

Algebraic security properties of DES

Theorem (1983 Even and Goldreich[3])

The one round DES functions generate the alternating group $\mathcal{A}_{\mathbb{Z}_2^{64}}$.

Theorem (1994 Coppersmith[4])

Let H *be the group generated by DES.* $|H| \geq 2^{2499}$.

[3] S. Even and O. Goldreich, "DES-like functions can generate the alternating group", *IEEE Transactions on Information Theory* (1983).

[4] D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks", *IBM Journal of Research and Development* (1994).

Algebraic security properties of DES

Theorem (1988 Kaliski, Rivest, and Sherman[5])

There is strong statistical evidence (due to cycling tests) that DES is not pure.

[5] B. S. Kaliski, R. L. Rivest, and A. T. Sherman, "Is the Data Encryption Standard a group?", *J. Cryptology* (1988).

DES over new groups

Theorem (2003 Patel, Ramzan, and Sundaram[6])

4-*round Luby-Rackoff ciphers over any group have* provable security *when the Feistel functions satisfy certain technical properties.*

[6] S. Patel, Z. Ramzan, and G. Sundaram, "Luby-Rackoff ciphers: why xor is not so exclusive", *SAC 2002, LNCS* (2003).

DES over new groups

Theorem (2003 Patel, Ramzan, and Sundaram[6])

4-*round Luby-Rackoff ciphers over any group have* provable security *when the Feistel functions satisfy certain technical properties.*

Problem

Let G be a finite group and $t \in \mathbb{N}$. When does DES over G^t form a group?

[6] S. Patel, Z. Ramzan, and G. Sundaram, "Luby-Rackoff ciphers: why xor is not so exclusive", *SAC 2002, LNCS* (2003).

DES over new groups

DES is a 16 round cryptosystem over $(\mathbb{Z}_2^{32})^2$.
Each round looks like

$$\sigma_i = \theta \circ \delta_{f_i}.$$

Definition

$\theta : (\mathbb{Z}_2^{32})^2 \to (\mathbb{Z}_2^{32})^2$: $\theta(x, y) = (y, x)$.

Definition

$\delta_{f_i} : (\mathbb{Z}_2^{32})^2 \to (\mathbb{Z}_2^{32})^2$: $\delta_{f_i}(x, y) = (x + f_i(y))$, where f_i is the *Feistel function* corresponding to the S-box with the ith subkey.

$$E_f = \theta \circ (\sigma_{16} \circ \cdots \circ \sigma_1).$$

DES over new groups

DES is a 16 round cryptosystem over $(\mathbb{Z}_2^{32})^2$.
Each round looks like

$$\sigma_i = \theta \circ \delta_{f_i}.$$

Definition

$\theta : (\mathbb{Z}_2^{32})^2 \to (\mathbb{Z}_2^{32})^2$: $\theta(x, y) = (y, x)$.

Definition

$\delta_{f_i} : (\mathbb{Z}_2^{32})^2 \to (\mathbb{Z}_2^{32})^2$: $\delta_{f_i}(x, y) = (x + f_i(y))$, where f_i is the *Feistel function* corresponding to the S-box with the ith subkey.

$$E_f = \theta \circ (\sigma_{16} \circ \cdots \circ \sigma_1).$$

DES over new groups

DES is an r round cryptosystem over $(G^t)^2$.
Each round looks like

$$\sigma_i = \theta \circ \delta_{f_i}.$$

Definition

$\theta : (G^t)^2 \to (G^t)^2$: $\theta(x, y) = (y, x)$.

Definition

$\delta_{f_i} : (G^t)^2 \to (G^t)^2$: $\delta_{f_i}(x, y) = (x + f_i(y))$, where f_i is the *Feistel function* corresponding to the S-box with the ith subkey.

$$E_f = \theta \circ (\sigma_r \circ \cdots \circ \sigma_1).$$

When is DES not a group?

Theorem

Let $\theta, \delta_f : G^{2t} \longrightarrow G^{2t}$ be defined as above. Then,

- *δ_f is an even permutation.*

When is DES not a group?

Theorem

Let $\theta, \delta_f : G^{2t} \to G^{2t}$ *be defined as above. Then,*

- δ_f *is an even permutation.*
- θ *is an odd permutation if and only if* $|G^t| \equiv 2, 3 \mod 4$.

When is DES not a group?

Theorem

Consider r round DES over G^{2t}. *If* $|G^t| \equiv 2, 3 \mod 4$ *and r is even, DES is not a group.*

When is DES not a group?

Theorem

Consider r round DES over G^{2t}. *If* $|G^t| \equiv 2, 3 \mod 4$ *and r is even, DES is not a group.*

Note

$|G^t| \equiv 2, 3 \mod 4$ *is equivalent to* $|G| \equiv 3 \mod 4$ *and t is odd or* $|G^t| = 2$.

The group generated by DES

Corollary

Let H be the group generated by r round DES over G^{2t}.
$H \not\leq \mathcal{A}_{G^{2t}}$ if and only if r is even and $|G^t| \equiv 2, 3 \mod 4$.

The group generated by DES

Problem

When does DES generate the full symmetric group?

[7] A. Maróti and M. C. Tamburini, "Bounds for the probability of generating the symmetric and alternating groups", *Arch. Math.* (2011).

The group generated by DES

Problem

When does DES generate the full symmetric group?

Theorem (2011 Maróti and Tamburini[7])

Let $\pi, \sigma \in \mathcal{S}_{\mathcal{M}}$ be random permutations and let $p(\mathcal{S}_{\mathcal{M}})$ be the probability they generate the symmetric group. Then, for $|\mathcal{M}| \geq 4$,

$$1 - \frac{1}{|\mathcal{M}|} - \frac{13}{|\mathcal{M}|^2} < p(\mathcal{S}_{\mathcal{M}}) \leq 1 - \frac{1}{|\mathcal{M}|} + \frac{2}{3\,|\mathcal{M}|^2}.$$

[7] A. Maróti and M. C. Tamburini, "Bounds for the probability of generating the symmetric and alternating groups", *Arch. Math.* (2011).

Simplified DES over elliptic curves

Simplified versions of DES over $\mathbb{Z}_2^n$:

- B-DES[8],
- S-DES[9].

As part of our research, we created a simplified standard for DES over an elliptic curve isomorphic to $\mathbb{Z}_3$.

[8] W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory* Ch. 4, Pearson Education, (2006).

[9] E. F. Schaefer, "A simplified Data Encryption Standard algorithm", *Cryptologia*, (1996).

Future work

- When is (generalized) DES pure?

Future work

- When is (generalized) DES pure?
- Other algebraic security properties.

Future work

- When is (generalized) DES pure?
- Other algebraic security properties.
- Can this same approach be used for other cryptosystems?

References

- K. W. Campbell and M. J. Wiener, "DES is not a group", *Advances in Cryptology—CRYPTO '92, LNCS* (2003).
- D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks", *IBM Journal of Research and Development* (1994).
- S. Even and O. Goldreich "DES-like functions can generate the alternating group", *IEEE Transactions on Information Theory* (1983).
- B. S. Kaliski, R. L. Rivest, and A. T. Sherman, "Is the Data Encryption Standard a group?", *J. Cryptology* (1988).
- A. Maróti and M. C. Tamburini "Bounds for the probability of generating the symmetric and alternating groups", *Arch. Math.* (2011).
- S. Patel, Z. Ramzan, and G. Sundaram, "Luby-Rackoff ciphers: why xor is not so exclusive", *SAC 2002, LNCS* (2003).
- E. F. Schaefer, "A simplified Data Encryption Standard algorithm", *Cryptologia*, (1996).
- W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory* Ch. 4, Pearson Education, (2006).
- L. Babinkostova, A. Bowden, A. Kimball, and K. Williams, "A simplified and generalized treatment of DES related ciphers", *submitted for publication*. arXiv:1205.5613v2 [math.GR]