Differential biases, c-differential uniformity, and their relation to differential attacks

Lukas Kölsch

University of South Florida

(joint work with Daniele Bartoli, Giacomo Micheli)

Differential uniformity

Definition

The DDT_F (difference distribution table) and differential uniformity δ_F of a function $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^n$ is defined as:

$$\mathrm{DDT}_F[a,b] = \#\{x \in \mathbb{F}_p^n \colon F(x+a) - F(x) = b\},$$
$$\delta_F = \max_{a \in \mathbb{F}_p^{n*}, b \in \mathbb{F}_p^n} \mathrm{DDT}_F[a,b].$$

The DDT tracks how differences propagate through a block cipher. A low differential uniformity is desirable.

Block ciphers and their round functions

Figure: An iterated (key-alternating) block cipher with r rounds and subkeys k_i that encrypts a plaintext m into a ciphertext c

The round function of a substitution permuation network (SPN)

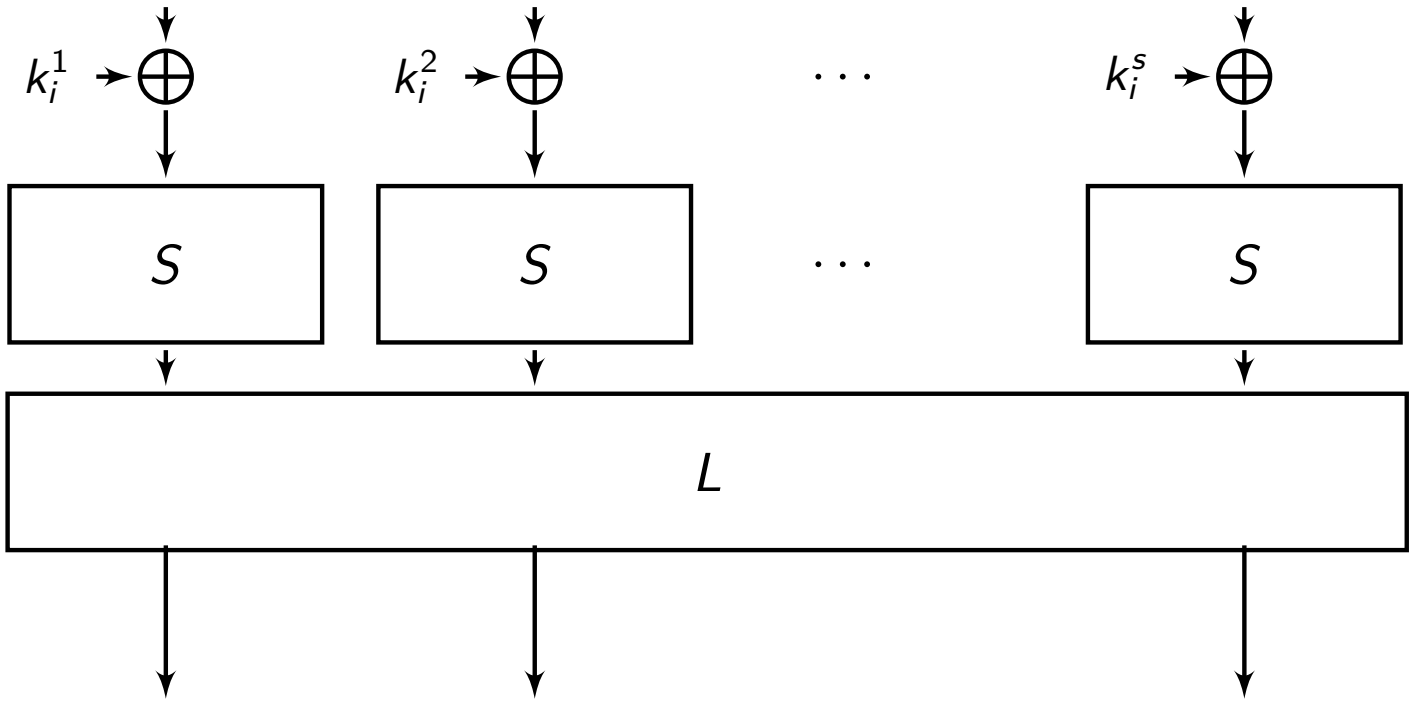

Figure: A high-level view of one round of an SPN with an S-box S, linear layer L and round key k_i

Differential attacks on SPNs

So an SPN consists of three steps that are repeated:

1. Key addition
2. S-box
3. Linear layer

Important: Differences are invariant under key addition:

$(x + a) + k - (x + k) = a$ and

$(F(x + a) + k) - (F(x) + k) = F(x + a) - F(x)$

..and the values of the DDT are invariant under the linear layer:

$L(x + a) - L(x) = L(x + a - x) = L(a)$.

So analysis can be broken down to the S-box level!

A generalization of the DDT

The following generalization was proposed in 2020 by Ellingsen, Felke, Riera, Stanica, Tkachenko.

Definition

Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, and $c \in \mathbb{F}_{p^n}$. For $a, b \in \mathbb{F}_{p^n}$, we let the entries of the c-Difference Distribution Table (c-DDT) be defined by ${}_c\,\mathrm{DDT}_F[a, b] = \#\{x \in \mathbb{F}_{p^n} : F(x + a) - cF(x) = b\}$. We call the quantity

$$ {}_c\delta_F = \max\{{}_c\,\mathrm{DDT}_F(a, b) \ : \ a, b \in \mathbb{F}_{p^n}, \text{ and } a \neq 0 \text{ if } c = 1\}$$

the *c-differential uniformity* of F.

This definition captures how the values $F(x + a) - cF(x)$ propagate through the cipher.

$c = 1$ is regular differential uniformity.

Question

Can the c-differential uniformity be used for a "differential attack-like" attack for values other than $c = 1$?
(Interestingly, there are no published papers on this so far...)

Question

There are many possible values for c. What kind of functions can have low c-differential uniformity for all values of c?

The first question

Question

Can the c-differential uniformity be used for a "differential attack-like" attack for values other than $c = 1$?

We saw for $c = 1$: Analysis can be broken down to S-boxes and is independent of the round key addition.

Does this translate to other values of c?

Key addition

$$(x + a) + k - c(x + k) = a + (1 - c)(x + k),$$

$$F(x + a) + k - c(F(x) + k) = F(x + a) - cF(x) + (1 - c)k.$$

so if $c \neq 1$ then the differences are dependent on the message x and the key k.

Makes analysis much harder (almost impossible?).

The linear layer

Let $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^n$.

Recall: $L(x+a) - L(x) = L(a)$ and

$L(F(x+a)) - L(F(x)) = L(F(x+a) - F(x))$so an attacker can control differences.

Identify $\mathbb{F}_p^n$ with $\mathbb{F}_{p^n}$. If L is linear over a subfield $\mathbb{F}_{p^k}$ then for all $c \in \mathbb{F}_{p^k}$:

$$L(x+a) - cL(x) = L(x+a-cx),$$

$$L(F(x+a)) - cL(F(x)) = L(F(x+a) - cF(x)).$$

But if $c \notin \mathbb{F}_{p^k}$ then this of course does not hold.

We investigate how composition with affine permutations affects the c-differential uniformity.

The linear layer

Theorem (BKM)

Let $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a function and $A\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be an affine permutation, where $A = L + s$ and L is the linear part of A. Then

$$ {}_c\mathrm{DDT}_F[a, b] = {}_c\mathrm{DDT}_{F\circ A}[L(a), b],\ {}_c\delta_F = {}_c\delta_{F\circ A}. $$

If L is linear over $\mathbb{F}_{p^l}$ where $l = [\mathbb{F}_p(c)\colon \mathbb{F}_p]$, then

$$ {}_c\mathrm{DDT}_F[a, b] = {}_c\mathrm{DDT}_{A\circ F}[a, A^{-1}(b)] $$

and

$$ {}_c\delta_F = {}_c\delta_{A\circ F}. $$

However, generally ${}_c\delta_F \neq {}_c\delta_{A\circ F}$ if $c \neq 1$.

The first question

Question

Can the c-differential uniformity be used for a "differential attack-like" attack for values other than $c = 1$?

Seems very hard since key addition and linear layers do not "communicate well" with c-differences in general. In particular, the analysis cannot be broken down to the Sbox level.

Even if biases exist (i.e. high c-differential uniformity for some c) it is unclear how to abuse this, unless $c = 1$.

Some potential maybe if linear layers are chosen as linear over subfields, or if $p > 2$ and $c \in \mathbb{F}_p$.

The second question

Question

There are many possible values for c. What kind of functions can have low c-differential uniformity for all values of c?

We look at functions $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ with low degree with respect to the field size p^n.

Functions with low degree allow tools from algebraic geometry/Galois theory to be used more easily (Weil bound, Galois groups).

The approach

We consider $G = F(x+a) - cF(x) - t \in \mathbb{F}_{p^n}(t)[x]$.
Roots of this polynomial (specified for some t) encode information on the solutions of $F(x+a) - cF(x) = t$.
If the degree of F is small, then (using for instance the Weil bound) we can guarantee that G behaves "regularly".
An important tool is the connection between the geometric and arithmetic Galois groups of G, i.e. the Galois groups over $\overline{\mathbb{F}_{p^n}}(t)$ and $\mathbb{F}_{p^n}(t)$.

- The geometric Galois group encodes splitting behavior over $\overline{\mathbb{F}_{p^n}}$, i.e. ramification,
- The arithmetic Galois group encodes splitting behavior over $\mathbb{F}_{p^n}$, i.e. number of solutions of $F(x+a) - cF(x) = t$.

- The geometric Galois group encodes splitting behavior over $\overline{\mathbb{F}_{p^n}}$, i.e. ramification,
- The arithmetic Galois group encodes splitting behavior over $\mathbb{F}_{p^n}$, i.e. number of solutions of $F(x+a) - cF(x) = t$.

If the degree is low enough, one can prove (under certain conditions) that the two groups coincide for most values of c, so the geometric behavior "determines" the number of solutions of $F(x+a) - cF(x) = t$.
The ramification bahavior can be studied purely algebraically using algebraic geometry methods.

Theorem

Let $q = p^n$, p a prime, and $F \in \mathbb{F}_q[x] \setminus \mathbb{F}_q[x^p]$, F not a monomial, with $d = \deg(F)$. Suppose that one of the following holds:

1. *$p = 2$, d is odd, and both the Hasse derivatives F' and F'' do not vanish;*
2. *$p > 2$ and $d \not\equiv 0, 1 \pmod{p}$.*

The number of $c \in \mathbb{F}_q$ for which ${}_c\delta_F < \deg(F)$ is bounded by an explicit constant B independent of q.

We can bound the constant by $B < 4d^2$.

So if d is small with regard to q and d satisfies the conditions, then F has *maximal* c-differential uniformity for *most* c.

What does this theorem mean?

We show that low degree functions generally will have bad c-differential uniformity (if conditions hold..).

Of course, for fixed field size q most functions have high degree, so we only considered a small subset of functions.

High level view: Biases are generally impossible to avoid! The big question is not if a bias exists, but if a bias can lead to cryptographic attack!

Conclusion

c-differential uniformity does not behave nicely with respect to linear layers and key addition compared to "regular differential uniformity". (As long as the way we do "key addition" does not change at least).

It is not clear how with the current ciphers, one would use high c-differential uniformity for an attack on an established cipher.

Theoretically, we have proven that a wide class of functions has provably high c-differential uniformity.

Postdoc positions open at University of South Florida (Tampa, FL)

Starting 08/2025, application will be possible around November 2024.
Check mathjobs.org in November.

Thank you for your attention!