HO DC and CUBE

Sort of "Algebraic" Attacks

"When Ciphers Have Low Degree"

HODC Lai, AIDA, Cube, Filiol, O'Neil Defectoscopy etc

Nicolas T. Courtois

- University College London

" Trivial – ε Attacks "

Cube attack are highly sophisticated highly technical attack BUT they achieve NOTHING more than breaking XX – ε rounds of a cipher where XX – ε rounds is already broken by an attack which crypto community considers as excessively trivial.

Boolean Functions, ANF

Any function $GF(2)^n \rightarrow GF(2)$.

Basics. Let $\mathcal{F}_n$ be the set of all functions mapping $\{0,1\}^n$ to $\{0,1\}$, $n > 0$, and let $f \in \mathcal{F}_n$. The *algebraic normal form* (ANF) of f is the polynomial p over GF(2) in variables $x_1, \ldots, x_n$ such that evaluating p on $x \in \{0,1\}^n$ is equivalent to computing $f(x)$, and such that it is of the form[3]

$$\sum_{i=0}^{2^n-1} a_i \cdot x_1^{i_1} x_2^{i_2} \cdots x_{n-1}^{i_{n-1}} x_n^{i_n}$$

for some $(a_0, \ldots, a_{2^n-1}) \in \{0,1\}^{2^n}$, and where i_j denotes the j-th digit of the binary encoding of i (and so the sum spans all monomials in $x_1, \ldots, x_n$)

Multivariate Cryptography:

Cryptosystems using polynomials with several variables over a finite field…

Multivariate Cryptanalysis or Algebraic Cryptanalysis:

Cryptographic attacks using polynomials with several variables over a finite field…

Roadmap: Multivariate/Algebraic Cryptanalysis

Guess Then Determine:
SAT/UNSAT strategy or mixed with many steps

MITM

Software / SAT Solvers

ElimLin: amazingly powerful

XL, Grobner Basis, F4, F5
dense systems of eqs, inappropriate tools in most other cases

Cube Attacks
[Vielhaber, Dinur,Shamir'08]

combination attacks

~~other tools~~

Truncated Differentials (DC)

Higher Order Differentials
"every cipher of low degree poly can be broken"

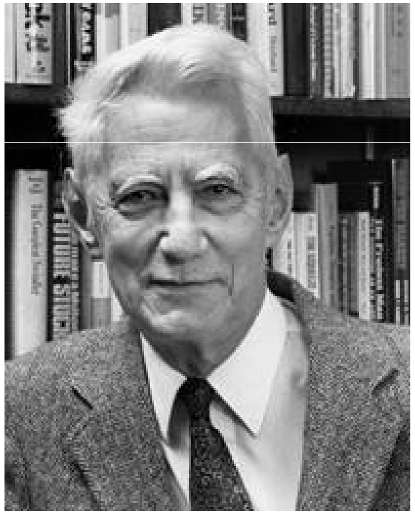
multiple points DC

Higher Order DC

Exact/Algebraic/Multivariate Cryptanalysis:

Breaking a « good » cipher should require:

“as much work as solving a system of simultaneous equations in a large number of unknowns
of a complex type”
[Shannon, 1949]



Common belief: large systems of equations become intractable very easily.

The Role of Finite Fields, e.g. GF(2)

They allow to encode any cryptographic problem as problem of solving Boolean equations.

MC = Definition

- Every function can be represented as a number of multiplications + linear functions over a finite field/ring.
- We call MC (Multiplicative Complexity) the minimum number of multiplications needed.

Home reading: set of slides multcomp.pdf Moodle.

**The Role of NP-hard Problems

Guarantee “hardness” in the worst case.

Many are not that hard in practice…

- Many concrete problems can be solved.
- Multiple reductions allow to use algorithms that solve one problem to solve another.

Algebraization:

Theorem:

Every function over finite fields is a polynomial function.

[can be proven as a corollary of Lagrange's interpolation formula] $P(X) = \sum_{i=1}^{t} Y_i \cdot \prod_{1 \le j \le t, j \ne i} \frac{X - X_j}{X_i - X_j}$

False over rings!

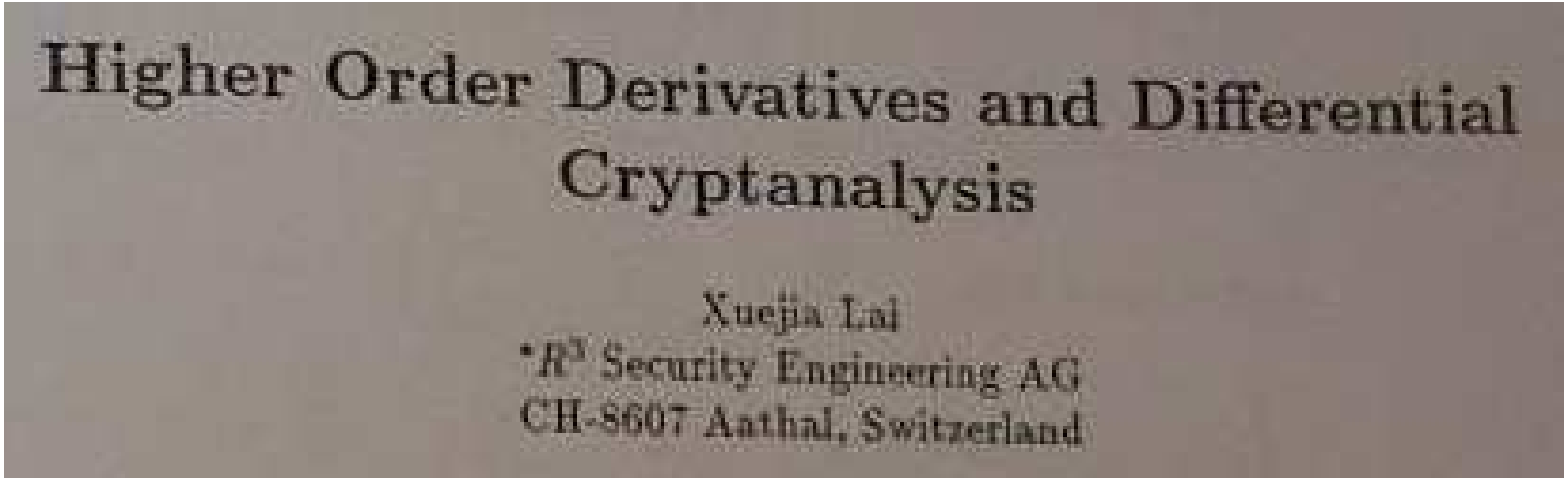
Problem 4: Low Degree/Low Complexity

Bottom line:

"Every cipher which can be expressed by low degree polynomials is broken."

Cf. Xuejia Lai paper.

- "Higher order derivatives and differential cryptanalysis" [1992]



Higher Order Derivatives and Differential Cryptanalysis

Xuejia Lai
*R^3 Security Engineering AG
CH-8607 Aathal, Switzerland

Problem 4: Low Degree/Low Complexity

Bottom line:

"Every cipher which can be expressed by low degree polynomials is broken."

Remark for LFSR-based stream ciphers:
later we will see how to substantially LOWER the degree…
I/O Relations, Algebraic Immunity, Annihilators, Courtois-Meier attack, etc…

Xuejia Lai – General Abelian Case

derivative

Definition Let $(S,+)$ and $(T,+)$ be Abelian groups. For a function $f : S \to T$, the *derivatives of f at point $a \in S$* is defined as

$$\Delta_a f(x) = f(x+a) - f(x).$$

i-th derivative

Note that the derivative of f is itself a function from S to T, we can define the *i-th* $(i > 1)$ *derivative of f at* $(a_1, a_2, \ldots, a_i)$ as

$$\Delta^{(i)}_{a_1,\ldots,a_i} f(x) = \Delta_{a_i}(\Delta^{(i-1)}_{a_1,\ldots,a_{i-1}} f(x))$$

where $\Delta^{(i-1)}_{a_1,\ldots,a_{i-1}} f(x)$ being the $(i-1)$-th derivative of f at $(a_1, a_2, \ldots, a_{i-1})$. The 0-th derivative of $f(x)$ is defined to be $f(x)$ itself.

Essential Result

Proposition 2 *Let* $\deg(f)$ *denote the nonlinear degree of a multivariable polynomial function* $f(x)$. *Then*

$$\deg(\Delta_a f(x)) \leq \deg(f(x)) - 1. \tag{17}$$

=> "Every cipher which can be expressed by low degree polynomials is broken."

Example. For

$$f(x_1, x_2, x_3, x_4) = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_2x_3x_4,$$

we compute the second derivative at (0001,1010).

$$\Delta_{0001} f(x_1, x_2, x_3, x_4) = f(x_1, x_2, x_3, x_4 \oplus 1) \oplus f(x_1, x_2, x_3, x_4) = x_1x_2 \oplus x_2x_3,$$

$$\Delta_{1010}(x_1x_2 \oplus x_2x_3) = x_2 \oplus x_2 = 0.$$

Binary Case

Binary functions in ANF,

group operation=XOR or \oplus in Latex.

bitwise XOR, denoted by $\oplus$.

Proposition 3 *Let $L[a_1, a_2, \ldots, a_i]$ be the list of all 2^i possible linear combinations of $a_1, a_2, \ldots, a_i$. Then,*

$$\Delta^{(i)}_{a_1, \ldots, a_i} f(x) = \sum_{c \in L[a_1, a_2, \ldots, a_i]} f(x \oplus c) \tag{18}$$

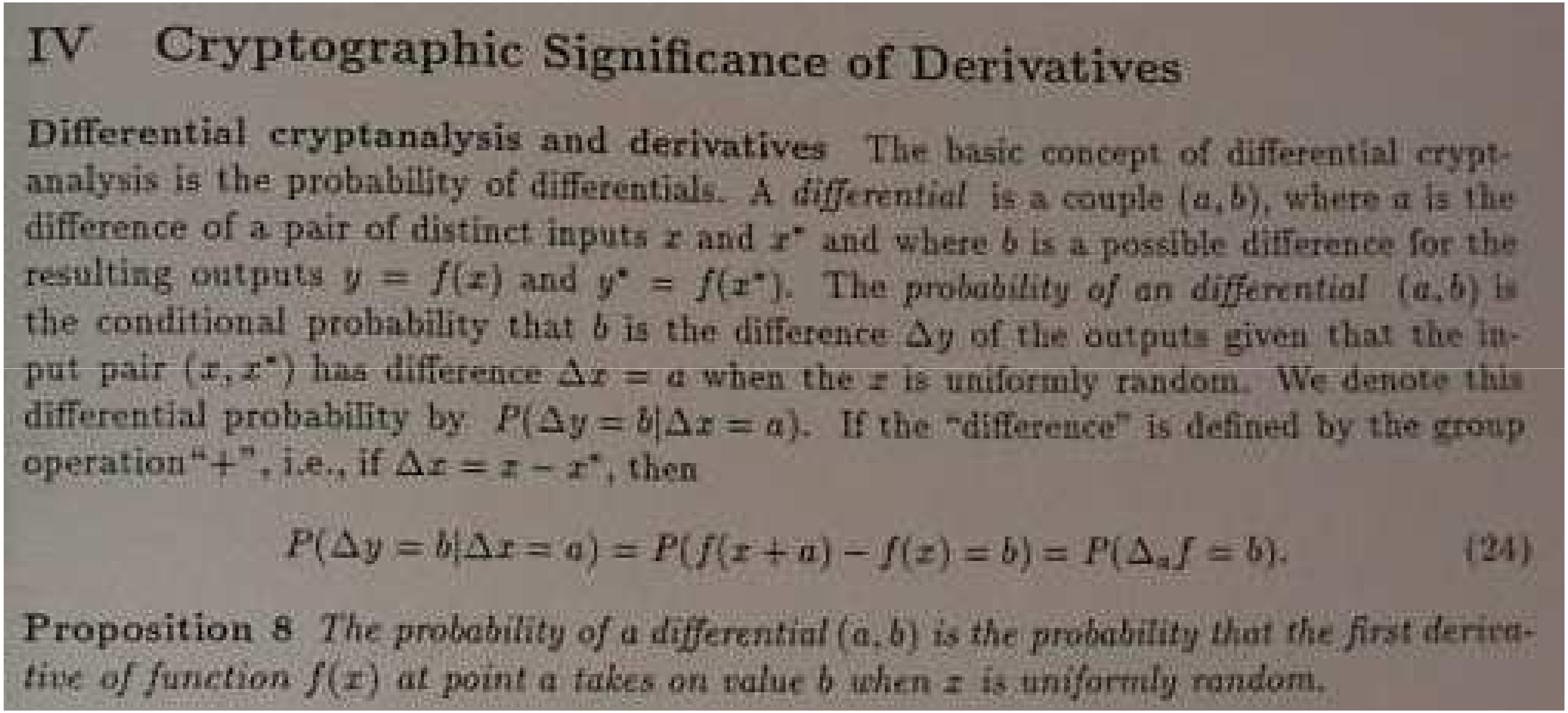
Corollary 4 *Derivatives of binary function is independent of the order in which the derivation is taken, i.e., for any permutation $p(j)$ of index j,*

$$\Delta^{(i)}_{a_1, \ldots, a_i} f(x) = \Delta^{(i)}_{a_{p(1)}, \ldots, a_{p(i)}} f(x) \tag{23}$$

Link to DC [Biham-Shamir]

Proposition 8 *The probability of a differential* (a, b) *is the probability that the first derivative of function* $f(x)$ *at point* a *takes on value* b *when* x *is uniformly random.*

*More Details



IV Cryptographic Significance of Derivatives

Differential cryptanalysis and derivatives The basic concept of differential cryptanalysis is the probability of differentials. A *differential* is a couple (a,b), where a is the difference of a pair of distinct inputs x and x^* and where b is a possible difference for the resulting outputs $y = f(x)$ and $y^* = f(x^*)$. The *probability of an differential* (a,b) is the conditional probability that b is the difference Δy of the outputs given that the input pair (x,x^*) has difference $\Delta x = a$ when the x is uniformly random. We denote this differential probability by $P(\Delta y = b|\Delta x = a)$. If the "difference" is defined by the group operation "+", i.e., if $\Delta x = x - x^*$, then

$$P(\Delta y = b|\Delta x = a) = P(f(x+a) - f(x) = b) = P(\Delta_a f = b). \quad (24)$$

Proposition 8 *The probability of a differential (a,b) is the probability that the first derivative of function $f(x)$ at point a takes on value b when x is uniformly random.*

Cube Attacks on Tweakable Black Box Polynomials

Itai Dinur and Adi Shamir

Computer Science depertment
The Weizmann Institute
Rehobot 76100, Israel

Cube Attacks

[Vielhaber, Dinur,Shamir'08]

Cube Testers and Key Recovery Attacks
On Reduced-Round MD6 and Trivium

Jean-Philippe Aumasson[1*], Itai Dinur[2], Willi Meier[1†], and Adi Shamir[2]

Step By Step

Cube attack is about summing COMPLEX multivariate polynomials.

Step By Step

Cube attack is about summing COMPLEX multivariate polynomials.

– most polynomials never written.

- Online phase CPA => several concrete values added 0+1+…
- Their sum polynomial depends on the key in a very simple way.

=>Gives simple equations on the key.

ANF of F(n variables)

$$\sum_{i=0}^{2^n-1} a_i \cdot x_1^{i_1} x_2^{i_2} \cdots x_{n-1}^{i_{n-1}} x_n^{i_n}$$

Basic observation: For any function, the sum (XOR) of all entries in the truth table:

$$\sum_{x \in \{0,1\}^n} f(x)$$

Equals to the coeff. of $x_1 x_2 \ldots x_n$ in ANF.

Example 4 Vars

$$f(x_1, x_2, x_3, x_4) = x_1 + x_1x_2x_3 + x_1x_2x_4 + x_3$$

Then summing $f(x_1, x_2, x_3, x_4)$ over all 16 distinct inputs makes all monomials vanish and yields zero, i.e. the coefficient of the monomial $x_1x_2x_3x_4$

Instead = Cube Attacks

- 2 sorts of variables secret/public.
- summing over well-chosen special subsets of inputs.

Instead = Cube Attacks

- 2 sorts of variables

Abstract. Almost any cryptographic scheme can be described by *tweakable polynomials* over $GF(2)$, which contain both secret variables (e.g., key bits) and public variables (e.g., plaintext bits or IV bits). The cryptanalyst is allowed to tweak the polynomials by choosing arbitrary values for the public variables, and his goal is to solve the resultant system of polynomial equations in terms of their common secret variables. In this paper we develop a new technique (called a *cube attack*) for solving such tweakable polynomials,

Sum Over Subsets - Example

$$f(x_1, x_2, x_3, x_4) = x_1 + x_1x_2x_3 + x_1x_2x_4 + x_3$$

Sum over 4 possible values of x_1 and x_2.

$$f(0,0,x_3,x_4) + f(0,1,x_3,x_4) + f(1,0,x_3,x_4) + f(1,1,x_3,x_4) = x_3 + x_4$$

Essential property:

$(x_3 + x_4)$ is the polynomial that multiplies x_1x_2 in f:

superpoly

$$f(x_1, x_2, x_3, x_4) = x_1 + x_1x_2(x_3 + x_4) + x_3$$

Some Sums Are More Interesting

- some hidden polynomials CAN be computed efficiently by the attacker.

superpoly

Basic Decomposition

Any subset I of $x_1 x_2 \ldots x_n$

master polynomial

$$f(x_1, \ldots, x_n) = t_I \cdot p(\cdots) + q(x_1, \ldots, x_n)$$

black-box

t_I = product of all vars in I

superpoly of I in f

poly only variables not in I

no monomial is a multiple of t_I

Key Lemma [Dinur-Shamir 2008]

sum polys over the cube t_I.

=> means vary inputs in I =>

$$\sum_{c \in L[a_1, a_2, \ldots, a_i]} f(x \oplus c)$$

cf. Lai HODC

$$\sum_I t_I \cdot p(\cdots) + q(x_1, \ldots, x_n)$$

only variables not in I

$$= \sum_I t_I \cdot p(\cdots)$$

$$= p(\cdots)$$

superpoly of I in f

- lower degre
- sometimes MUCH lower!!!!!!

Some Sums Are More Interesting

- Some hidden polynomials CAN be computed efficiently by the attacker.

superpoly

- And for some ciphers these polynomials are VERY interesting (they allow key recovery).

Pre-Computation

- Interesting sets I and interesting output linear combinations are found by "black box probing".
    - Polynomials are NEVER written
    - Mostly impossible to write down: by far too large…

Which Sums Are So Interesting?

- Unusually low degree.

superpoly of I in f

$$= p(\cdots)$$ lucky => linear

- A cube t_I is called a maxterm IF it has degree 1 (linear).

Which Sums Are So Interesting?

- Unusually low degree.

superpoly of I in f $= p(\cdots)$

•Linear:
mix of key and plaintext variables or similar!!!!!!

- The attacker COMPUTES/RECONSTRUCTS the linear superpoly by assuming that it is linear and findign out the coefficients.
  - Greedy algo, super large I => sum constant [cf. Lai HODC] => make I smaller => repeat => be lucky..
  - not key-dependent, they are just polynomials true for every key

Online Phase - CPA

- Now secret k_i variables are fixed, we can VARY public variables.

$$\sum_I f(x_1, \ldots, x_n)$$

superpoly of I in f $= p(\cdots)$

gives 1 linear equation on key bits!!

- If size of I is d => at most 2^d CP are needed.

*Cube Controversies

Cube Attacks Controversies [1]

Dan Bernstein: http://cr.yp.to/cubeattacks.html

- "Why haven't cube attacks broken anything?

actually it broke a VERY large number of rounds of Trivium

- Cube attacks work well for random polynomials of small degree.
  - Real-world ciphers, when viewed as polynomials, don't have small degree.
  - Lai 1992 explains how to break **every** small-degree cipher;
  - It seems to me that "cube attacks" are simply a reinvention of Lai's HO DC attack; if Dinur and Shamir had cited Lai's paper […] then they would have been forced to drop essentially all of their advertising.

*Cube Controversy [2]

Plagiarism:

- Dinur and Shamir DO/DID NOT credit Michael Vielhaber's "Algebraic IV Differential Attack" (AIDA) as a precursor of the Cube attack.
  - Dinur has stated at Eurocrypt 2009 that Cube generalises and improves upon AIDA.
- However, Vielhaber contends that the cube attack is no more than his attack under another name.

*Cube Controversy [3]

- Actually Dinur-Shamir's paper takes it much further. It is a landmark paper in history of cryptanalysis.
  - General, generous practical and far reaching.
    - » In spite of plagiarism issues.
- I think everybody [Lai,Berstein,Vielhaber] FAILED to see that the real innovation in the Cube attack are computational SHORTCUTS:
  - to compute certain combinations of polynomials CHEAPER than by any previously known method…
    - Wikipedia: Cube [attack] uses an efficient linearity test […] results in the new attack needing less time than AIDA, although how substantial this particular change is remains in dispute.
  - It is not the only way in which Cube and AIDA differ.
    - Vielhaber claims, for instance, that the linear polynomials in the key bits that are obtained during the attack will be unusually sparse.

Cube Testers

See Chapter 7 in Aumasson PhD thesis and his paper with Dinur Shamir etc…