New Frontiers in Symmetric Cryptanalysis

Nicolas T. Courtois
University College of London, UK

Are Cryptologists Always Wrong?
Neal Koblitz: Yes!

[…] Once I heard a speaker from NSA complain about university researchers who are cavalier about proposing untested cryptosystems. He pointed out that in the real world if your cryptography fails, you lose a million dollars or your secret agent gets killed.
In academia, if you write about a cryptosystem and then a few months later find a way to break it, you’ve got two new papers to add to your résumé![…]

Feel Secure or Paranoid Today?

Optimistic View
Nothing bad has ever happened.

Anybody ever broke DES in practical sense?

The Curious “Science” of Security

“We need – today again -- to re-discover the frontiers of what is secure that have just moved yesterday…

Claim:
The cryptographic research alone is changing so much that some serious thinking is needed now to see what it is and what it should be about.
**Fundamental Research:**

Claim:
Some most fundamental questions that pertain to more or less all symmetric cryptosystems were never seriously studied.

**Current Bets:**

I encourage people to propose new bets related to their own research.

**Can one Reconcile Paranoia and Security?**

Claim: we need yet to discover what is hard and what is not.

=>

I propose a new tool to help researchers making honest and responsible statements:

=> Bets on the future attacks.

**Frontiers**

1. Maths vs. Crypto
Science vs. Fiction

**New Tool - Bets**

For the first time in history, it is possible to bet on cryptographic algorithms with real money.

This has never been possible before.


Purpose: have fun and show the advancement of cryptographic research. It is a game.

**Science vs. Fiction**

Laws of Prediction [Arthur C. Clarke]:
When a distinguished elder scientist tells you something is not possible => he is wrong...

Algebraic Attacks on AES/Serpent/Etc:
“Provably” Secure [2000]
=> Speculative Fiction [2001]
=> Science Fiction [2002]
=> Science [2004-7]
=> Reality ??
**What Can Said About Frontiers**

They are natural: people from one place will naturally have trouble understanding other people.

- Some people come from **Pure Orthodox Mathematics**
- Some people are in **Information Security**
  - Cryptology/Computer Science/Law/ Crime Science/Finance and Economics/Marketing/Sociology/…

**Cryptology**

Ignorance Trap:
- We do **NOT WANT TO KNOW** about attacks unless:
  - They are faster than other known attacks on the same cipher (why so? major fallacy)
  - Their importance is already widely recognised (conservatism)

Also unless:
- It breaks their cipher, not ours…
- You pay us consultancy fees for that…

**Very Recent Paper**

Neal Koblitz:

“The Uneasy Relationship Between Mathematics and Cryptography”,
In Notices of the American Mathematical Society, September 2007, see [www.ams.org](http://www.ams.org)

Cryptographic community:
- “The “spy vs. spy mentality”
- “constant competition and rivalry”
- “excessive - and even childish at times”

**Mathematics**

Intelligence Trap:
- **Applied maths** is bad maths.
- We do not want to consider facts.
  - We want to study ONLY what is provable [+ with our favourite tools].
    - Control freak?
  - Zero risk: Do not dare formulate a conjecture that is not true.
  - Cryptology: 60% risk for experts, 99% for beginners.
- We have a proof, we don’t need to experiment to verify if it’s true.
  - Many proofs are actually wrong, subtleties.
- We need to study attacks that are complex and clever.
  - Simple attacks are not interesting?

**Mathematics [overheard]**

- Mathematics: direct relationship with God.
- This **cryptology** is a profane and stupid engineering science…
- Cryptologists =def= people that have not grown big enough to do maths.

**Mathematics vs. Cryptology**

- Some mathematicians are maybe studying the empty set.
  - There are specific examples: Inaccessible cardinals, Ramsey cardinals, etc…

- In cryptology we do it ALL the time. Conjectured assumptions collapse on a daily basis.
Cryptology:
- Cryptology is almost a separate “science” that defines its own object of study (formal security definitions).
- We need to add axioms to mathematics.
  - Not everything is provable, statements that we love to make are all like: \( \forall \text{algorithm} \).
  - Very few such statements were ever proven and very few will ever be...

Frontiers:
- Frontiers are natural...
- We do not need to create extra artificial frontiers
  - Natural ones are enough trouble!

Remark:
“The discourse regarding the role of complexity in cryptography has degenerated to a point where it may take some time to recover.”
[Kevin McCurley, in post about Kobitz’s criticism of crypto, 14 Sept. 2007]

Cryptologic Community:
Not much is proven...

and many things will never be.

A group of people with shared beliefs
- Some deeply rooted in a certain reality of hardness resulting from precisely this endless confrontation of clever designers and clever attackers...
- Some are spectacularly naïve and are to collapse next, as usual in cryptology.
  - Like a religion in which the Gospels are rewritten each year.

AES
Advanced Encryption Standard:
- In 2000 NIST selected Rijndael as the AES.
But in late 2001
A new kind of “terrorist” appears and strikes some basic certitudes.

AL – GEB – RA
الجبير

So far the terrorist he has not been captured and might strike again from his secret basement.

Maybe:
Mathematical certitudes are an ideal to look up to...

But:
Let’s keep feet on the ground.

Frontierology:
Frontiers are opportunities for discovery and exploration.

2. Algebraization, New Frontier in Symmetric Cryptography?

Two Religions [Maths and Crypto]
We will not agree on some questions any time soon...  
Goal: learn each other’s language.

Mathematics

Cryptography

MQ Problem
Find a solution to a system of $m$ quadratic equations with $n$ variables over a field/ring.
Cryptography and MQ

Claim: 95% of all applied cryptography depends on the hardness of MQ.
1. RSA is based on MQ with \( m = 1 \) and \( n = 1 \): factoring \( N \) \( \Leftrightarrow \) solving \( x^2 = C \bmod N \).

Universality/completeness:
any polynomial system can be written as quadratics with added variables...

MQ Problem

Multivariate Version

[\( n \) variables]

MQ Problem over GF(2)

Find a solution (at least one), i.e. find \( (x_0, \ldots, x_{n-1}) \) such that:

\[
\begin{align*}
1 & = x_1 + x_0 x_1 + x_0 x_2 + \ldots \\
0 & = x_1 x_2 + x_0 x_3 + x_7 + \ldots
\end{align*}
\]

More Applications of MQ

1. Public key schemes based on MQ directly, e.g. HFE [broken by Courtois, Joux and Faugère] and Sflash [broken by Stern, Shamir et al.]
2. If sparse MQ is easy, any block cipher including AES should be easy to break...
3. Dense MQ is VERY hard. In 2006 Patarin et al. propose QUAD, a provably secure stream cipher based on MQ directly.
   - Open problem: propose a provably secure block cipher

Jean Dieudonné

[French Mathematician]
Book “Calcul infinitésimal”, Hermann, 1980

[…] Everybody in mathematics knows that going from one to several variables is an important jump that is accompanied by great difficulties and calls for completely new methods. […]

Schneier [Applied Cryptography book]

[…] Any algorithm that gets its security from the composition of polynomials over a finite field should be looked upon with scepticism, if not outright suspicion. […]

Written before AES ever existed...

Actually any cipher can be seen in this way…
Algebraization:

Theorem:
Every function over finite fields is a polynomial function.

False over rings!
  E.g. false for F-functions.

Cryptology:

Since the 70s mathematics started conquering cryptology. Before cryptography meant “bad mathematics” [Koblitz].

Since the early 2000s, algebra is “conquering” cryptanalysis of ciphers, in order for:
- Algebraic public-key, like HFE [late 90s].
- Symmetric ciphers with algebraic components:
  - stream ciphers, AES.
- Now, algebraization of ciphers that have no algebraic structure AT ALL, such as DES
  [Courtois-Bard, IMA Cryptography and Coding 2007 and eprint.iacr.org/2006/402].

What Can Said About Frontiers

Frontiers move:

The process can be called CONQUEST.
- Not always pejorative.

Any Progress?

Not many block ciphers are broken so far…

Some are:
KeeLoq, used by millions of people every day to open their cars, can be broken by an Algebraic Attack in practice.

Algebraization:

Mathematics:
Since, say the second half of XIX-th century, algebra is “conquering” other areas of mathematics. E.g.
- Algebraic Topology
- Algebraic Geometry
- Etc..

The Role of Finite Fields

They allow to encode any cryptographic problem as problem of solving Boolean equations.
**The Role of NP-hard Problems**

Guarantee “hardness” in the worst case.

Many are not that hard in practice…
- There is hope and many concrete problems can be solved.
  - Multiple reductions allow to use algorithms that solve one problem to solve another.

---

**Symmetric Cryptanalysis:**

From what one can observe:

- **bad news:**
  - number of ciphers “broken w.r.t. claims”:
    - \(O(\text{effort})\).

- **good news:**
  - number of ciphers “broken in practice”:
    - \(o(\text{effort})\).

---

**Algebraization:**

- Algebraic Topology
- Algebraic Geometry
- Etc…

Works both ways, algebraic problems can also be viewed in geometric terms.

**Example:** Theory of T-functions is actually about ultra-metric Non-Archimedean geometry over 2-adic integers.

So maybe the “connection” will strike back!

---

**3. New Territory: Algebraic Attacks on Ciphers**

---

**Algebraization => Geometry-isation?!**

Maybe now geometry may help to bring the topic of solving algebraic equations forward?

- Interesting new topics in cryptanalysis of symmetric ciphers to be studied now.

**Maybe it is probably all already known in mathematics and we [cryptanalysts] just didn’t realise it was there and can be applied to build efficient algorithms to solve systems of equations…**

This is already done in number-theory based crypto: LLL is the “geometry of numbers” approach.

---

**How Serious is Cryptanalysis?**

Do expect:

- some nice research results in algebraic cryptanalysis
  - 0 casualties.

BTW: We will discover that this no different from LC/DC/Etc. We will also work on “metric of relative interest” of cryptographic attacks.
Propose New Ciphers?

Foolish, requires lots of courage:

# Ciphers “broken w.r.t. claims” = \( O(\text{effort}) \).

Algebraic Cryptanalysis of Block Ciphers?
Also foolish, requires lots of courage:
so far EXCESSIVELY POOR results,
progress is slow. \( O(\text{effort}) \)?

Two Worlds:

- The “approximation” cryptanalysis:
  - Linear, differential, high-order differential, impossible differential, Jakobsen-Knudsen approximation, etc.
  - All are based on probabilistic characteristics true with some probability.
  - Consequently, the security will grow exponentially with the number of rounds, and so does the number of required plaintexts in the attacks (main limitation in practice).
- The “exact algebraic” approach:
  - Write equations to solve, true with probability 1.
  - Very small number of known plaintexts required.

Algebraic Cryptanalysis [Shannon]

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]

What’s New?

CLAIM:
The two worlds CANNOT be compared.

They are going in a very different direction:
what these two CAN ACHIEVE in practice are two very rich sets of cryptanalytic results that are rather disjoint.

Motivation

Linear and differential cryptanalysis usually require huge quantities of known/chosen plaintexts.

Q: What kind of cryptanalysis is possible when the attacker has only one known plaintext (or very few)?

Claim: This question did not receive sufficient attention. Misguided focus on LC and DC.

Terra Incognita

…two sets of cryptanalytic results that are rather disjoint.

=> So we are really discovering a new frontier for the whole of symmetric cryptanalysis.
**Symmetric Cryptanalysis:**

*Problem:* current metrics for achievement in symmetric cryptanalysis is deeply flawed. For example:

$2^{13}$ KP is NOT better than $2^{56}$ and 1 KP. DES was never really broken.  
[Don Coppersmith, Crypto 2000].

---

**Real-life Security Metrics:**

\[2^{70} = 2^{20}\]

An attack with $2^{70}$ is worth as much as with $2^{20}$ operations as both are feasible (!).

Compare these two attacks ONLY on:
- the number of required plaintexts
- KP/CP/CPCA etc.

$=>$ Then, an algebraic attack in $2^{70}$ is worth as much as a differential attack in $2^{20}$ operations...

---

**Algebraic Attacks vs. DC/LC/etc..**

- Algebraic attack in $2^{70}$ operations
  - $=>$ the only feasible in the real life !
- Attacks with $2^{50}$ memory – infeasible.
- LC in $2^{20}$ operations – infeasible.
  - Hard to get $2^{20}$ KP !
- DC in $2^{20}$ operations – infeasible.
  - Hard to get $2^{20}$ CP !

---

**Major Fallacy:**

**Gets worse - Remark:** by assuming that $2^{13}$ KP is feasible (it isn’t) block ciphers have too many rounds. Paranoid approach.

As a consequence, attacks that are really feasible, e.g. $2^{70}$ and 4 KP are never studied.

---

**Therefore:**

- Computing power is the CHEAPEST resource. Should NO LONGER BE be the comparison metrics.
- Running time comparison with LC/DC is dishonest, makes little sense and should be avoided.

---

**What to Expect from Algebraic Cryptanalysis**

As much as from LC/DC/Etc.:
- Drop hope for practical attacks on AES for now…
- Goal: Just to advance research in symmetric cryptanalysis: what ciphers can be broken, how, and why.
A Strategic Problem
Are they dead bodies in the closet?
- Expect that a couple of insecure ciphers exists under the cover of industrial/military secret.
  - Lightweight ciphers, designed some time ago, etc.
  - Don’t expect me to break them. I don’t have the spec.
- These will eventually come out... but for now we need to find substitutes to break – so that there is some progress in cryptanalysis!
- ECRYPT ESTREAM project: ciphers grown under “glass house”.
  - Goal: make sure that ciphers are broken before being used, and not the opposite...

This was Stream Ciphers.
What About **Block Ciphers**?

Phil Rogaway Talk:
‘obviously we cannot found a scientific theory based on what people DO NOT know’
Later he says:
=> “Can take a human-ignorance approach for formalising properties of [...] blockciphers, etc.”

Better hardness (classical) may be replaced by assuming ignorance?

Maybe P = NP (there are fast algorithms) but they are hard to find/invent, and not hard to run.

Research in Symmetric Cryptanalysis

Question (C0): what ciphers can be broken.
Claim: This is an incorrect and misleading question.
Existence doesn’t mean we can find them...

Better Formulation (Code Constructive or C1): What ciphers we (with our ignorance, background and available tools), can break in the next 50 years (and how?).

“Glass House” for Algebraic Attacks of Block Ciphers

Web site dedicated to cooperation in algebraic cryptanalysis:
- Publish a system of equations that describe important practical ciphers [e.g. DES].
- Make other researchers compete in solving these.
- See where is the frontier: limitations of these attacks
  => new effective measure of security.
www.cryptosystem.net/aes/toyciphers.html

See Phil Rogaway:
Formalizing Human ignorance: Collision-Resistant Hashing without the Keys
eprint.iacr.org/2006/281

Question (C0): what ciphers can be broken.
Claim: This is an incorrect and misleading question.
Existence doesn’t mean we can find them...
What Ciphers We Can Break
(with our ignorance, background and available tools...) in the next 50 years?

Well, it depends also what ciphers we WANT/TRY to break.
- The most precious resource is time and attention of clever people. Results will greatly depend on how this resource is being allocated. Ciphers that get attention are much more likely to be broken.
- Another scarce resource: CPU time and willing to experiment a lot... Maybe hardness is not where you think.

More Powerful Approach

Claim: many attacks will never be discovered if you do not experiment.

Experimentation

Theory

Fact

There are powerful tools that break certain ciphers without anybody knowing exactly why and when they work. (Cumulative effect of different phenomena that we can study separately).

The source code is usually not public. Non trivial implementation problems. E.g.

\[
tiny\text{subset}(F4) >> \text{one version of F4} >> \text{another F5}.
\]

Tools – black-box (cryptanalytic oracles).

Weakness of Cryptographic Research Community

In fundamental physics, there are people that do the theory, and other people that design and handle experiments for their whole life.

Claim: we need this in symmetric crypto.

Otherwise we are not doing a lot of progress and are lying to everybody about some systems being not broken...
Symmetric Crypto

Statistical Cryptanalysis:
Successful \( \Rightarrow \) More rounds are considered \( \Rightarrow \)
Scarcity of attacks as only few combinations of biases give sufficiently strong overall bias.

Algebraic Cryptanalysis:
At present time: a handful of rounds, yet over-abundance of attacks to try.
MANY degrees of freedom.

Frontiers
4. Sources of Algebraic Vulnerability

Paradigm Shift
[Shannon, Jakobsen-Knudsen, Patarin, Pieprzyk-Courtois et al]
- Look at multivariate algebraic relations (implicit equations).
- Claim: This is the most general formulation of algebraic attacks [Carlet’s Algebraic Immunity (AI) is a very, very restricted one].

Unified view of Algebraic Attacks
- Non-existence of small multivariate relations between inputs/outputs:
  - Applies to multivariate public key crypto-systems, Sihash, Quartz
  - Applies to the non-linear part of a stream cipher, even if stateful
  - Applies to the S-boxes of a block cipher

Nicolas Courtois: General Principles of Algebraic Attacks and New Design Criteria for Components of Symmetric Ciphers,
In AES 4 Conference, LNCS 3373, Springer.

Def: “I / O Degree” = “Graph AI”
Consider function \( f : \mathbb{G}(2)^n \to \mathbb{G}(2)^m \),
\( f(x) = y \), with \( x = (x_0, \ldots, x_{m-1}) \), \( y = (y_0, \ldots, y_{m-1}) \).

Definition [The I/O degree] The I/O degree of \( f \) is the smallest degree of the algebraic relation
\( g(x_0, \ldots, x_{m-1} ; y_0, \ldots, y_{m-1}) = \Omega \)
that holds with certainty for every couple \( (x, y) \) such that \( y = f(x) \).

Design of Ciphers
When people design block cipher they usually study “ALL KNOWN ATTACKS” on it, then claim that the system is resistant to them.

My conjecture: it has become HARD to know and maybe THERE IS NO WAY to know, if a given system is resistant to all known attacks [particularly difficult for algebraic attacks].
From S-F to Reality

Laws of Prediction [Arthur C. Clarke]:
When a distinguished elder scientist tells you something is not possible => he is wrong...

Algebraic Attacks on AES/Serpent/Etc:
“Provably” Secure [2000]
=> Speculative Fiction [2001]
=> Science Fiction [2002]
=> Science [2004-7]
=> Reality ???

Sources of Algebraic Vulnerability

There are two!

Two Sources of Algebraic Vulnerability

2 “crazy” conjectures [Courtois]:
- I/O Degree Hypothesis (IOH): all ciphers with low I/O degree and lots of I/O relations are broken when the number of rounds is not too large.
- The Very Sparse Hypothesis (VSH): ciphers with very low gate count are broken when the number of rounds is not large.

Break AES ?

Until recently, excessively poor results...
How far are we now?
- Maybe we go in a completely different direction.

BUT... Caution is required.
- So far there is no such thing like “algebraic immunity”, just algebraic vulnerabilities. “Instability theory”.
- Too many new attacks are still waiting to be discovered just by trying them.

***My Program:

- Forget AES. It doesn’t make a lot of sense to work on AES or on reduced versions of it. You do not progress by approaching problems from the hard side. Approach the problem from the easy side.
- Do attack stream ciphers such as Snow, toy block ciphers, etc.
- Do NOT LOOK if they are secure against other attacks. Comparison with LC/DC makes no sense.
- Do experiment a lot. Do develop tools.
- Mistake I made: Do NOT think that very sophisticated tools developed by other people (e.g. F5) are very useful...

What Can be Done?

Algebraic Cryptanalysis:
- Very special ciphers: 1 M rounds [Courtois’AES4].
- General ciphers, key size=block size: SMALL number of rounds, 4,5,6 rounds.
  - Nobody can break CTC2(255,255,7).
- If key size > block size – more rounds.
  - CTC2(96,256,10) can be broken.
- If many solutions (Hash functions, MACs) => expected to be still easier.
What is Hard?
The complexity of current attacks does grow VERY QUICKLY with the number of rounds.
  • Like 100x for each additional round...

So
  • no hope for breaking full Serpent = 32 rounds
  • Fact: 5 rounds Serpent is quite weak w.r.t.
    algebraic attacks, unlike 4-bit Rijndael S-box.

Algebraic Attacks on Block Ciphers

Gröbner Bases, XL:
  • How to avoid reduction to 0 while increasing the
degree of polynomials.
  • Mostly infeasible in practice...

Claim: A lot of research in a wrong direction.
  There are many much better methods to break
  ciphers. They are NOT more advanced/more
  sophisticated. On the contrary, they are much
  simpler.

Fast Algebraic Attacks on Block Ciphers

Definition [informal on purpose] Methods to lower the degree
of equations that appear throughout the computations...[e.g. max deg in F4]

How to lower the degree?
  • use several Pic pairs (bigger yet much easier!)
  • by clever choice of representation
  • by CPA
  • by adding well-chosen constraints
  • etc...

ElimLin

Later today.

One Example

The biggest discoveries in
Science are the simplest.

ElimLin

Complete description:
  • Find linear equations in the linear span.
  • Substitute, and repeat.

Amazingly powerful, huge systems collapse
with no effort.
E.g. breaks 5 rounds of DES given 3 KP.
See eprint.iacr.org/2006/402/
**ElimLin – Something Wrong?**

Q1. Why do we have linear equations in the first place?

- Stupid in mathematics...
- IMPOSSIBLE TO AVOID in cryptanalysis.
  - E.g. take several KP.
  - Add well-chosen constraints
  - Etc.

**ElimLin – Still A Bit Weird Feeling**

Q2. Why don’t we eliminate them?

- First answer, if we do, we lose sparsity and the capacity to compute anything at all.
- Second answer: we do, but then NEW LINEAR EQUATIONS appear. “Avalanche effect”.
  - Quite surprising.
  - Can go quite far.
  - Additional tricks can help to re-launch the “avalanche” process that gets stuck...

---

**CTC2**

- Virtually no difference
  - Much stronger against LA
  (cf. Dunkelman-Keisar attack).

---

**CTC2 Cipher**

Equations generating program now available
www.cryptosystem.net/see/toycipher.html

---

**CTC = “Courtois Toy Cipher” [eprint]**

- 3-bit S-boxes.
- Diffusion D: permuting wires (as DES P-box).
- 1,2,4,8,... S-boxes per round.
- 1,2,3,...10, ...30,... rounds.
- Key size == Block size.
- Simple key schedule: bit permutation (as in DES 1).

---

**Attacks on CTC2**

- key size == block size:
  - I can break up to 6 rounds.
  - Current frontier: nobody can break CTC2(255,255,7). Can anybody? Please try!

- If key size > block size
  => more rounds.
  - CTC2(96,256,10) can be broken.
Gröbner Bases Soon to be Forgotten?

Not at all, but attention must be shifted from high degree [all work on F5] to handling much bigger systems but at a very low degree (in a sense less than 2).

Algebraic Attacks

Or maybe other attacks?

- Attacks on DES with SAT solvers [6 rounds].
- Raddum-Semaev attacks.
  - Claimed best, only 4 rounds.

Claim

Many hard problems (breaking ciphers) rely on very easy mathematical problems (e.g. sparse linear algebra) but applied to huge systems of equations.

This requires completely new tools. Equations have to be compressed and stored on disk, but then they have to be manipulated in completely new ways so that the computation is done smoothly.

All algorithms for these "easy" problems have to be redone, use algebraic properties to "rearrange" the order of computations...
3.4. ANF-to-CNF - The Outsider

Convert MQ to a SAT problem.
(both are NP-hard problems)

Fact:
Sparse random MQ can be broken in practice, some in seconds.

Works for any system of equations - if sparse enough and/or over-defined enough...

This has never been shown before.

Results on DES
Nicolas T. Courtois and Gregory V. Bard: “Algebraic Cryptanalysis of the D.E.S.”.

In IMA Cryptography and Coding 2007
eprint.iacr.org/2006/402/

At a first glance,
Seems pointless:

there is no strong algebraic structure
of any kind in DES

What Can Be Done?

Attack 1: CNF Representation + Minisat:
We recover the key of 6-round DES with 3 KP faster than brute force.
• When 23 variables fixed, takes 175 s.
  • Magma crashes 2 Gb of RAM.

Attack 2: Optimised Gate-level representation + our
ANF-to-CNF conversion+ MiniSat 2.0:
Key recovery for 6-round DES. Only 1 KP (!).
• Fix 20 variables takes 6 s.
  • Magma crashes with > 2 Gb.
Frontiers
6. Limitations of Algebraic Cryptanalysis

Some limitations of algebraic cryptanalysis are very hard, we "hit the wall" (e.g. when the number of rounds increases).

Some are spectacularly naïve (e.g. maximum degree in Gröbner basis computation) and are easily circumvented.

DES – New Frontier:
Break 8 rounds
given 1 KP and in less than $2^{55}$.

We encourage researchers to try.
We cannot do it so far.

What Are the Limitations of Algebraic Attacks?
• When the number of rounds grows:
  complexity jumps from 0 to $\infty$.

• With new attacks and new “tricks” being proposed: some systems are suddenly broken with no effort.
  $\Rightarrow$ jumps from $\infty$ to nearly 0!