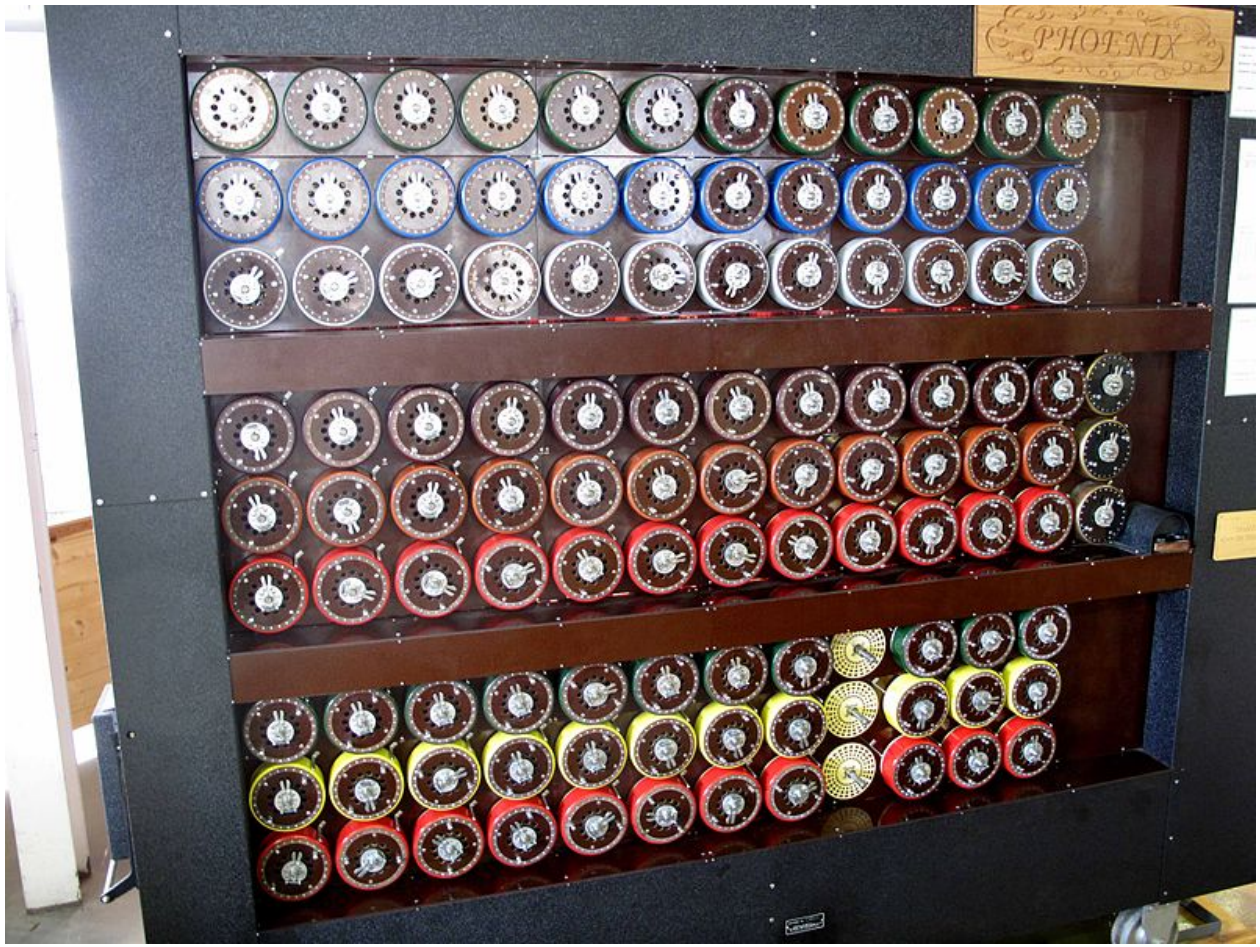
Cryptanalysis vs. Reality
+
Small Cryptanalysis

Jean-Philippe Aumasson

http://131002.net @aumasson

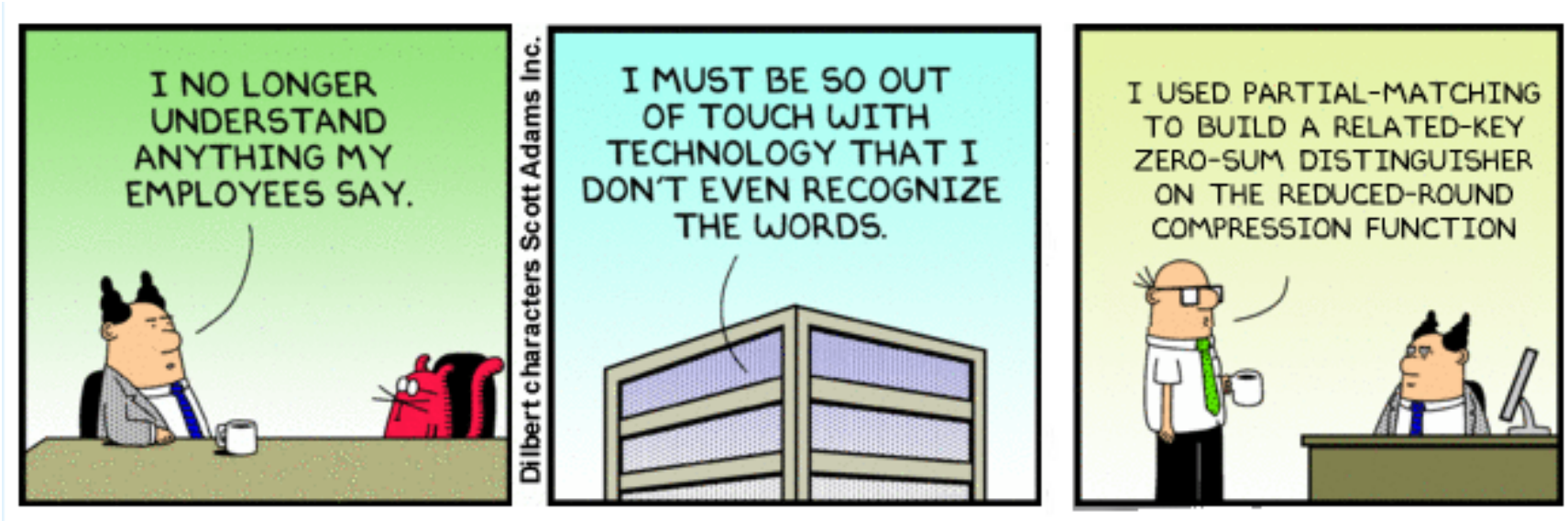
NAGRAVISION
KUDELSKI GROUP

Cryptanalysis used to be connected to reality



(replica of a Turing's bombe used to break Enigma during WWII)

But times have changed



How does cryptanalysis affect real-world security?

Focus on symmetric cryptanalysis of

- Block ciphers
- Stream ciphers
- Hash functions
- PRNGs
- MACs

Do not consider attacks on public-key encryption/signatures, authentication protocols, etc.

In this talk: cryptanalysis = algorithmic attacks

“cryptanalysis usually excludes methods of attack that do not primarily target weaknesses in the actual cryptography, such as bribery, physical coercion, burglary, keystroke logging, and social engineering”
(“Cryptanalysis” in Wikipedia, 15.06.11)

Also excludes

- Weak-RNG attacks (Sony PS3, OpenSSL, etc.)
- Side-channel attacks (DPA etc.)
- Fault attacks
- Etc.

= attacks that do break crypto in reality?

Examples of (non-) attacks on deployed primitives

High-complexity attacks

Attacks on building blocks

Related-key attacks

Time, memory, data

Distinguishers

(Un)predictable attacks

Example from pay-TV

Conclusion

Null- to low-impact attacks (examples)

- A5/1: practical attacks on GSM essentially bruteforce
- AES: high-complexity related-key attacks
- DES: bruteforce remains the most powerful attack
- SHA1: collision attack below 2^{70}, unverified
- GOST: recent attacks , best attack still codebook
- Whirlpool: distinguisher for the compression only
- Triple DES: safe for 112-bit security

Medium- to high-impact attacks (examples)

- WEP/RC4: break of WEP exploits RC4 biases
- MD5: famous rogue certificate attack PoC
- AES cache-timing attacks (e.g. on OpenSSL)
- Padding oracle attacks (IPsec, ASP.net, RoR, etc.)
- TEA equivalent keys exploited in Xbox hack

Unattacked primitives (examples)

- CAST-256
- Grain80
- IDEA
- IDEA-NXT
- Twofish
- Serpent
- RIPEMD-160

Many attacks, but the situation is not so bad. . . why?

High-complexity attacks

Example: $2^{123.4}$ preimage attack on MD5 (Sasaki/Aoki)

Reduces the security level from n-bit to $(n - \varepsilon)$-bit

Does not matter in practice as long as a break remains unfeasible/unlikely (e.g. 256 to 220 bits, but not 128 to 80)

*“ The difference between 80 bits and 128 bits of keysearch is like the difference between a mission to Mars and a mission to Alpha Centauri. As far as I can see, there is *no* meaningful difference between 192-bit and 256-bit keys in terms of practical brute force attacks; impossible is impossible.”* (John Kelsey)

Attacks on building blocks

E.g. attacks on the compression function in a hash, attacks on the block cipher in a compression function

Example: 2^{96} collision attack on LANE's compression

- Did not lead to an attack on the hash
- Invalidates the security reduction compression$\prec$hash
- Disqualified LANE from the SHA3 competition

Like reduced-round attacks, can be interpreted as a failure to attack the full primitive. . .

Related-key attacks

Attackers learn encryptions with a derived key $K' = f(K)$

One of the first attacks: when Enigma operators set rotors incorrectly, they sent again with the correct key...

Modern version introduced by Knudsen/Biham in 1992

Practical on weak key-exchange protocols (EMV, 3GPP?), but unrealistic in most decent protocols

Tentative Formalization by Bellare/Kohno, Albrecht et al., to exclude generic attacks (AND/OR attack, etc.)

Related-key attacks example

2^{119} key-recovery on AES-256 (Biryukov/Khovratovich)

Needs 4 related keys

Relations given in terms of subkey relations

“attacks are still mainly of theoretical interest and do not present a threat to practical applications using AES”

Time, memory, data

Previous example attacks:

- MD5: time $2^{123.4}$ and 2^{50}B memory (1024 TiB)
- LANE: time 2^{96} and 2^{93}B memory
- AES: time 2^{119} and 2^{77}B memory

Practical cost of access to memory accesses neglected

Should compare to (parallel) bruteforce with similar hardware (equivalent “size”? price in $?)

Memory (storage) distinct from data (queries)

Inconsistent time units (bit op, “query”, Sbox call)

Time, memory, data

Example: recent attacks on GOST (Courtois/Misztal):

- GOST $\approx$ Russian DES
- 256-bit key, 64-bit block
- Key-recovery in time 2^{226},
- Needs store all 2^{64} plaintext/ciphertext's

Codebook attack needs same 2^{64} data and memory, but no extra computation

Should we bother finding the key then? (as it is an "encoding" of the codebook)

In some cases yes, e.g. when key update $K := H(K)$ is used to ensure backward secrecy

Distinguishers

a.k.a. distinguishing attacks

Used to be statistical biases in keyed primitives

Now distinguishers are often

- Known- or chosen-key
- Sets of input/output's satisfying some relation

Example: differential q-multicollision distinguisher on AES

$$\begin{aligned} E_{K_1}(P_1) \oplus E_{K_1 \oplus \Delta}(P_1 \oplus \nabla) &= E_{K_2}(P_2) \oplus E_{K_2 \oplus \Delta}(P_2 \oplus \nabla) \\ &= \cdots \\ &= E_{K_q}(P_q) \oplus E_{K_q \oplus \Delta}(P_q \oplus \nabla) \end{aligned}$$

Distinguishers: extreme example

The SHA3 candidate Keccak uses a permutation

$$\text{Keccak-}f : \{0,1\}^{1600} \rightarrow \{0,1\}^{1600}$$

Keccak's proof of indifferentiability (from a RO) makes the assumption that Keccak-f admits no distinguisher

"Zero-sum" distinguishers for P were found

- in 2^{1023} on 16-round (Aumasson/Meier)
- in 2^{1590} on the full 18-round (Boura/Canteaut)

Due to these results, Keccak-f now has 24 rounds

Distinguishers: definitions?

No standard general rigorous definition of a distinguisher

“You know what I mean attacks” (Joan Daemen)

The problem (simplified):

- A dist’er does something that’s infeasible with a similar effort for an ideal primitive
- Like finding multicollisions, partial preimages, etc.
- Ideally it is hard to find a preimage of

```
8d550afedbdf6c4d569a5dd2e3a8e2c8704046...
```

yet I know one for SHA-256. . .

Distinguishers vs. reality

Marginal impact in applications

Cryptanalysts do not choose to find distinguishers rather than (say) collisions, it's just sometimes the best we find

Serve to compare the "absolute strength" of algorithms (ideally, no distinguisher should exist)

Proved useful to disqualify candidates from the SHA3 competition and to publish papers

(Un)predictable attacks

Example of predictable attacks: differential attacks

- Determine the probability of following a characteristic
- Infer the possibility of an attack in (say) 2^{110}

Example of unpredictable attacks:

- Attacks using SAT solvers, algebraic solvers
- Cube attacks

Complexity determined empirically, extrapolation difficult

Have guarantee that unpredictable attacks do work

Naive differential analysis can give too optimistic or pessimistic complexity estimates (SHA1, KASUMI)

Example from pay-TV

DVB standard uses the Common Scrambling Algorithm (CSA) to encrypt video streams (e.g. MPEG2 TS packets)

CSA1/2: 48- to 64-bit key, cascade block+stream cipher

Useful break of CSA needs

- recover a key in $<$10 sec ("cryptoperiod")
- ciphertext-only, partially-known plaintext (no TMTO)

CSA3 standardized in 2007: 128-bit key, includes AES...

Conclusion

Cryptanalysis seldom breaks real-world systems, due to

- High complexity
- Large memory requirements
- Unrealistic models (related keys. . .)
- Attacks that are not attacks (distinguishers. . .)

“We don’t break ciphers, we evaluate their security”
(Orr Dunkelman)

- Does cipher X really provide 256-bit security?
- Risk of an attack in 30 years?

“Attacks always get better, never worse” (Bruce Schneier)

Related works

Leakage-resilience models vs. Reality

- Are models realistic? When?
- Standaert et al. “Leakage Resilient Cryptography in Practice” `http://eprint.iacr.org/2009/341`

Bruteforce vs. Reality

- What’s the real cost of bruteforce?
- Kleinjung et al. “Using the Cloud to Determine Key Strengths” `http://eprint.iacr.org/2011/254`

Crypto libs vs. Reality

- OpenSSL, Crypto++ et al. vs. physical attacks
- Junod “Open-Source Cryptographic Libraries and Embedded Platforms”
  `http://crypto.junod.info/hashdays10_talk.pdf`

Small Cryptanalysis

Joint work with
María Naya-Plasencia
Markku-Juhani O. Saarinen

KLEIN(e) Cryptanalysis

Joint work with
María Naya-Plasencia
Markku-Juhani O. Saarinen

KLEIN

Lightweight block cipher family by Gong, Nikova, Law

Presented at RFIDsec 2011 on June 27!

64-bit block, 64-, 80- 96-bit key versions

A round:

AddRoundKey	(XOR with a round key)
SubNibbles	(nibbles are 4-bit-Sboxed)
RotateNibbles	(2-byte state rotate)
MixNibbles	(2 MixColumn's in //)

KLEIN $\approx$ "Serpndael"

KLEIN differential analysis

Differential cryptanalysis is the main class of attacks used against symmetric crypto primitives

Security against differential attacks is typically proven by showing lower bounds on the probability of a differential characteristic

Theorem: Any 4-round differential characteristic of KLEIN has a maximum probability of 2^{-30}

KLEIN differential analysis

Differential cryptanalysis is the main class of attacks used against symmetric crypto primitives

Security against differential attacks is typically proven by showing lower bounds on the probability of a differential characteristic

Theorem: Any 4-round differential characteristic of KLEIN has a maximum probability of 2^{-30}

To bypass this bound, we used a collection of characteristics

- 4 rounds with probability 2^{-16}

1	SubNibbles RotateNibbles MixNibbles	□□ □□ □■ □□ □■ □□ □□ □□ □■ □■ □■ □■	□□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□	$2^{-0.42}$
2	SubNibbles RotateNibbles MixNibbles	□■ □■ □■ □■ □■ □■ □□ □□ □■ □■ □■ □■	□□ □□ □□ □□ □□ □□ □■ □■ □■ □■ □■ □■	$2^{-4.82}$
3	SubNibbles RotateNibbles MixNibbles	□■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■	□■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■	$2^{-10.64}$
4	SubNibbles RotateNibbles MixNibbles	□■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■	□■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■	$2^{-16.45}$
5	SubNibbles RotateNibbles MixNibbles	□■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■	□■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■	$2^{-22.27}$
6	SubNibbles RotateNibbles MixNibbles	□■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■	□■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■	$2^{-28.08}$
7	SubNibbles RotateNibbles MixNibbles	□■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■	□■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■ □■	$2^{-33.89}$

KLEIN differential analysis

8-bit MixColumn + 4-bit Sbox. . .

If nibble differences have the same MSB, MixNibbles gives

$$\texttt{0X0X0X0X0X0X0X0X} \mapsto \texttt{0X0X0X0X0X0X0X0X}$$

RotateNibbles preserves nibbles alignment

Let's exploit associated collections of characteristics. . .

Exploiting the differential

The attack

- Make chosen-plaintext queries to detect a good pair
- Use neutral bits technique to generate more pairs
- Divide-and-conquer approach to recover key bits

Key recovery on 8 rounds with complexity 2^{32}

Practical attack, experimentally verified

Working on possible extensions to 9+ rounds. . .

Conclusion

Attack on 8 rounds of KLEIN (12 rounds in total)

Small Sboxes and nibble alignment expose the cipher to high-probability differentials

Serpent's Sbox and Rijndael's MixColumn don't get along

Work in progress...

Cryptanalysis vs. Reality
+
Small Cryptanalysis

Jean-Philippe Aumasson

http://131002.net @aumasson