The Security of Lightweight Crypto Algorithms

Orhun Kara
Lightweight crypto algorithm

Information security with restricted resources

Restricted resources

- Area
  - Hardware
    - ≈1000-2000 GE
  - Software
    - 8 bit microprocessors
    - 1-2 KB ROM and RAM

- Power consumption
  - RFID tags

- Energy consumption
  - Mobile devices
  - Sensor networks

Lightweight Crypto Day 2016 TCE
Area

22 nm Tri-Gate Transistor

In 1 mm² 10 millions transistor

2-input 1 NAND gate = 1 GE
Area

Roughly 10.000 GE area
2.000 GE of it for security

RFID tag
Area: examples

Area & security

- AES (SHA 256/10)
- NTRU (EC 166/10)
- (EC 192)/10
- KTANTAN
- SIMON
- PRESENT
- LBlock
- TRIVIUM
- Grain
- PHOTON
- PRINTEGRITY
- LED
- DESL

Security x 10  Area in HW GE
Area in software

![Area in software diagram](image)

**Software Area for Various Algorithms**

- AES
- Camellia
- ITUBee
- KATAN
- DESL
- PRESENT
- Trivium

*Security X 10, ROM, RAM*
Power consumption

\[ P = \left( \frac{1}{2} \cdot C \cdot V_{dd}^2 + Q_{sc} \cdot V_{dd} \right) \cdot f \cdot N + I_{leak} \cdot V_{dd} \]

Like a sloth
Energy consumption per bit pJ

- KATAN
- AES-S
- AES_P
- LED
- PRINCE
- KLEIN_S
- KLEIN_P
- PRESENT

energy consumption pJ/bit
Stream ciphers vs block ciphers

Block cipher designs in last decade:

Area in HW

Power consumption

Block ciphers are the champions!
<table>
<thead>
<tr>
<th>Year</th>
<th>Block Cipher</th>
<th>Stream Cipher</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>Hight, mCrypton</td>
<td>Grain</td>
</tr>
<tr>
<td>2007</td>
<td>Clefia, PRESENT, DESL</td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>Mickey, Trivium</td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td>Katan/Ktantan</td>
<td>FCSR</td>
</tr>
<tr>
<td>2010</td>
<td>GOST revisited, PRINTCipher</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>LBlock, Picolo, LED, TWINE</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Klein, PRINCE</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>ITUBee, Simon, Speck, Zorro</td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>PRIDE</td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td></td>
<td>Sprout</td>
</tr>
</tbody>
</table>
Block cipher vs Stream cipher

0.13 or 0.18 µm

<table>
<thead>
<tr>
<th>Cipher</th>
<th>GE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trivium</td>
<td>2600</td>
</tr>
<tr>
<td>Grain</td>
<td>1294</td>
</tr>
<tr>
<td>Mickey</td>
<td>3600</td>
</tr>
<tr>
<td>LED</td>
<td>966</td>
</tr>
<tr>
<td>Ktantan</td>
<td>462</td>
</tr>
<tr>
<td>Simon</td>
<td>763</td>
</tr>
<tr>
<td>PRINTCipher</td>
<td>503</td>
</tr>
</tbody>
</table>

Why are block ciphers more compact?

TMD Tradeoff attacks:

- k bit security => roughly 12k GE register cost

<table>
<thead>
<tr>
<th>Bit</th>
<th>GE</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>960</td>
</tr>
<tr>
<td>128</td>
<td>1536</td>
</tr>
</tbody>
</table>

Power Consumption µW

- KATAN
- KTANTAN
- PRESENT
- DESXL
- PRINCE
- Grain
- Trivium

Power Consumption

Lightweight Crypto Day 2016 TCE
Generic weaknesses

- Short block length
  32/48 bit, code book
- Short key length
  40, 48, 64, 80 bit key
- Tradeoff attacks
  Hellman or rainbow tables
- Related key attacks
  Designers mostly ignore
- Side channel attacks
  Severe threat
- Structural weaknesses
  So many things to learn
Key length: Brute force attack

• 80 bit short (for a standard), 48 bit too short!

Hellman:
- The first thing we'd like to hit is the key size of the proposed standard. We feel it's too small, both today - we feel it's vulnerable to attack by an agency such as NSA. If you have $20,000,000 to invest in a machine, you could break the proposed algorithm by exhaustive search in one day's time.

Art (from NSA):
- Marty, Dana Grub, one of the engineers, made a study on produced figures that were quite at variance with yours, and instead of one day he gets something like 91 years.


EFF DES Cracker, 250,000 $, 1998; 56 hours
Short key length

Basic arithmetic: 80-56=24 bits
24×1.5=36;

Moore Law: breaking 56 bit in 1976 has the same cost as breaking 80 bit in 2012

Moreover: Lightweight algorithms are more efficient on special platforms such as COPACOBANA: More cores, no key schedule, high frequency, short block length etc.

<table>
<thead>
<tr>
<th></th>
<th>KLEIN</th>
<th>AES</th>
</tr>
</thead>
<tbody>
<tr>
<td>AREA</td>
<td>2500</td>
<td>20.000</td>
</tr>
<tr>
<td>FREQUENCY</td>
<td>500 MHz</td>
<td>300 MHz</td>
</tr>
<tr>
<td>ROUND N.</td>
<td>12</td>
<td>10</td>
</tr>
</tbody>
</table>
Tradeoff attacks

- First: Hellman tables DES, 1980
- Stream ciphers: Golic and Babbage, 1997
- Hellman tables of (variable and secret) internal states: Biryukov and Shamir, 2000

32 bit block length, 80 bit key
m=2^{48} , t=2^{32} ; 2^{80} key in the table

3.5 PB memory, whole codebook and 264Encryption => key recovery

Same numbers with chosen plaintext attack
Hellman table: Ubiquitous usage

80 bit key

One table: $m=2^{48}, t=2^{16}$
2.5 PB memory
$2^{64}$ offline computation
$2^{16}$ encryption per key and
One key recovery for each $2^{32}$ encryption (one in every $2^{16}$ key)
chosen plaintext attack!
Hellman table: Fair approach

<table>
<thead>
<tr>
<th>Key</th>
<th>IV</th>
<th>Internal States</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Keystream: $z_0, z_1, z_2, \ldots$</td>
</tr>
</tbody>
</table>

One way map from key to keystream for fixed IV

Security limits of tradeoff attacks for block ciphers:
- Offline phase: As expensive as brute force
- Online phase > $2^{2k/3}$

So, for stream ciphers: number of internal states should be at least $2^{4k/3}$ to have the same limits!
- Offline phase: Faster for BG tradeoff but it is possible to limit data
- Online phase > $2^{2k/3}$
Another approach: noisy keystream encryption

- Use \([n,k]\) linear code to encode the plaintext
- The error set has \(2^{n-k}\) errors
- TMD tradeoff attacks are error nontolerant
- No advantage on any linear combination or decimation of coordinates of error vectors
- Tradeoff between transmission rate and area
- The new internal state size will be \(2/(2-R)\); \(R\) information rate
- \([24,12]\) code, ratio is 1.33
- Additional cost of encoding & decoding
Another approach: fixed key

- Already known, but no practical application
- First practical example: Armknecht and Mikhalev FSE 2015: Sprout
- No condition on the internal state size

DEF (FSE 2015): A keystream generator (KSG) with Keyed Update Function (KUF) consists of the following functions:
An update function $F : K \times S \rightarrow S$ such that $F_k : S \rightarrow S$ is bijective for any $k$
An output Boolean function $G : S \rightarrow GF(2)$
$K = GF(2)^k$ is the key space and $S = GF(2)^s$ is the internal state space.
Keystream generator with keyed update function

**DEF:** A KSG with KUF is a clockwise shift registered KSG with KUF if

- for each call of the output function $G$, the update function $F$ is called once
- $F(K, S) = (S_1, S_2, \ldots, S_{s-1}; f_F(K; S))$ where $S = (S_0, \ldots, S_{s-1})$ and $f_F$ is the feedback Boolean function.

**DEF:** A state is weak internal state of order $m$ if one can generate $m$-bit output using the internal state alone without knowing the key.

Let the first output including $f_F(K; S)$ be of the form $f_F(K; S)h(S)$. Then the probability

$$ Pr_D = \text{Prob}(h(S)=1) $$

is called the probability of determining feedback (forward or backward).

Moreover, the probability

$$ Pr_G = \frac{1}{2} + |\text{Prob}(f_F(K,S)=1 | S)| - \frac{1}{2} |$$

is called the guess capacity.
Attacking to weak states

Offline Phase:
Load all the weak states of order m into a table with their outputs

Internal State Recovery Phase
For a weak state:
- Check if the next feedback value is determined from output (with $Pr_D$)
- Else check the state and if it survives guess the feedback from KUF (with $Pr_G$)
- Continue on so until the candidate state is eliminated
- The only candidate surviving will be the right state

Key Recovery Phase
Solve the key values in the feedback equations:

\[
\begin{align*}
    f_F(K; S^{(1)}) &= S_{s-1}^{(2)} \\
    f_F(K; S^{(2)}) &= S_{s-1}^{(3)} \\
    f_F(K; S^{(3)}) &= S_{s-1}^{(4)} \\
    \ldots
\end{align*}
\]
An example: Sprout

- 80 bit key, 80 bit register
- Grain type
- \( Pr_D = 1 \) for backward direction and \( Pr_D = 1/2 \) for forward direction
- \( Pr_G = 3/4 \) for some states and \( Pr_G = 1/2 \) for others
- Load weak states of order \( d+3 \) with the outputs: \( 2^{86-d} \)
- For each state, check the related keystream, \( 2^d \) data
- For \( d=40 \): 320 TB memory and \( 2^{40} \) bit keystream, \( 2^{33} \) encryption
Offline phase

For weak states of order $d+3$:

- $d-20$ nonlinear eqn’s with 60 unknowns
- Linearize and solve them
- Low sampling resistance
- $2^{42}$ system of linear equations with 20 unknowns for $d=40$
Another Attack!

“All Another Tradeoff Attack on Sprout-Like Stream Ciphers”
By Bin Zhang and Xinxin Gong, Asiacrypt 2015

Well, indeed the same attack with extra condition on weak states and output

<table>
<thead>
<tr>
<th>Attack</th>
<th>Data</th>
<th>Memory(-bit),(TB)</th>
<th>Time</th>
<th>Pre-computation</th>
</tr>
</thead>
<tbody>
<tr>
<td>[12]</td>
<td>112</td>
<td>$2^{52.32}$-bit, $\geq 639$ TB</td>
<td>$2^{66.80}$</td>
<td>$2^{68.87}$</td>
</tr>
<tr>
<td>[8]</td>
<td>$2^{40}$</td>
<td>$2^{52.58}$-bit, 770 TB</td>
<td>$2^{30.66}$</td>
<td>$2^{54.29}$</td>
</tr>
<tr>
<td>[8]</td>
<td>$2^{41}$</td>
<td>$2^{52.64}$-bit, 399 TB</td>
<td>$2^{29.66}$</td>
<td>$\approx 2^{56.70}$</td>
</tr>
<tr>
<td>[8]</td>
<td>$2^{42}$</td>
<td>$2^{50.69}$-bit, 207 TB</td>
<td>$2^{28.66}$</td>
<td>$\approx 2^{59.07}$</td>
</tr>
<tr>
<td>[8]</td>
<td>$2^{43}$</td>
<td>$2^{49.74}$-bit, 108 TB</td>
<td>$2^{27.66}$</td>
<td>$\approx 2^{61.42}$</td>
</tr>
<tr>
<td>ours</td>
<td>$2^{39}$</td>
<td>$2^{51.39}$-bit, 336 TB</td>
<td>$2^{40.66}$</td>
<td>$2^{44.03}$</td>
</tr>
<tr>
<td>ours</td>
<td>$2^{40}$</td>
<td>$2^{50.63}$-bit, 198 TB</td>
<td>$2^{39.66}$</td>
<td>$2^{43.39}$</td>
</tr>
<tr>
<td>ours</td>
<td>$2^{41}$</td>
<td>$2^{49.85}$-bit, 115 TB</td>
<td>$2^{38.66}$</td>
<td>$2^{43.81}$</td>
</tr>
<tr>
<td>ours</td>
<td>$2^{42}$</td>
<td>$2^{49.03}$-bit, 65 TB</td>
<td>$2^{37.66}$</td>
<td>$2^{45.36}$</td>
</tr>
<tr>
<td>ours</td>
<td>$2^{43}$</td>
<td>$2^{48.20}$-bit, 36 TB</td>
<td>$2^{36.66}$</td>
<td>$2^{47.09}$</td>
</tr>
</tbody>
</table>

“… $2^{10}$ times faster than Esgin/Kara attack [8] with much less memory”
So, still open!

So, there has been still no secure ultra lightweight stream cipher (say, less than 1K GE) yet

New approaches?
New criteria?
New designs?
Industry has a bad grade: GSM
Industry has a bad grade: GSM

- A5/1, A5/2:
  - Tradeoff attacks, rainbow tables
- Comp128
  - Collision attack: 130K challenge
Industry has a bad grade

- **Keeloq**
  - 32 bit block 64 bit key
  - $2^{16}$ chosen plaintext, practical attack Eurocrypt 2008
  - Side channel, power analysis: key recovery in one minute, factory key recovery in one day; Ruhr University Bochum

- **Hitag2**
  - Immobilizer security
  - 48 bit stream cipher
  - COPACOBANA: 2 hours
  - SATSolver on PC 7 hours
  - Gone in 360 seconds: $2^{35}$ operations; USENIX’12

---

Hitag2 Cipher

\[
\begin{align*}
f_a^4 &= 0x2C79 = abc+ac+ad+bc+a+b+d+1 \\
f_b^4 &= 0x6671 = abd+acd+bcd+ab+ac+bc+a+b+d+1
\end{align*}
\]
Industry has a bad grade

- **Crypto-1**
  - Mifare, contactless card
  - 48 bit key, LFSR filtering
  - Algebraic attack: 200 seconds on PC. “The security of this cipher is therefore close to zero”

- **DST40**
  - Immobilizer, Exxon-Mobil Speedpass paying systems
  - 40 bit key, unbalanced Feistel
  - Information Security Institute: Reverse engineering and brute force on FPGA 11 hours, John Hopkins University 2005
  - COPACOBANA: 9 minutes.
Industry has a bad grade

- **OMA MAC**
  - Open Smart Grid Protocol (OSGP), Energy Service Network Association (ESNA), ETSI standard
  - 96 bit key, same as encryption
  - 4 challenge and $2^{25}$ computation: Key recovery FSE 2015

- **E0**
  - Bluetooth, 128 bit key, combining LFSRs
  - Conditional correlation attack $2^{23}$ frame and $2^{38}$ encryption, Crypto 2005
As a result

- Key length: 64 bit, 80 bit, at least 96 bit

- Security assumptions are important
- Side channel resistance is necessary
Fifth International Workshop on Lightweight

http://lightsec16.akse1aray.edu.tr/tr

Sep 21-22, 2016

Aksaray University, Cappadocia / Turkey

Important Dates

Submission deadline: June 24, 2016
Acceptance notification: July 29, 2016
Final version due: August 19, 2016

General Chair
Atilla Elçi

Program Chair
Andrey Bogdanov
Questions?

Thank you..