Breaking Industrial Ciphers at a Whim

MATE SOOS

PRESENTATION AT HES'11

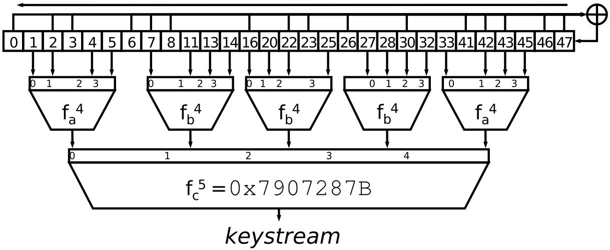
SECURITY
RESEARCH
LABS

Story line

1. HiTag2: reverse-engineered proprietary cipher
2. Analytic tools are needed to investigate them
3. CryptoMiniSat: free software tool to test ciphers (and to break them)

Philips HiTag2 Cipher

- For access control: cars, army buildings
- Proprietary: reverse-engineered by Karsten Nohl and Sean O’Neil



$$f_a^4 = \texttt{0x2C79} = abc+ac+ad+bc+a+b+d+1$$

$$f_b^4 = \texttt{0x6671} = abd+acd+bcd+ab+ac+bc+a+b+d+1$$

- Feedback linear(!), filter non-linear

SAT Solvers

Input: CNF, an “`and` of `or`-s’

- $(x_1 \vee \neg x_3) \quad \wedge \quad (\neg x_2 \vee x_3) \quad \wedge \quad (x_1 \vee x_2)$
- Crypto-problem needs conversion

Uses DPLL(φ) algorithm

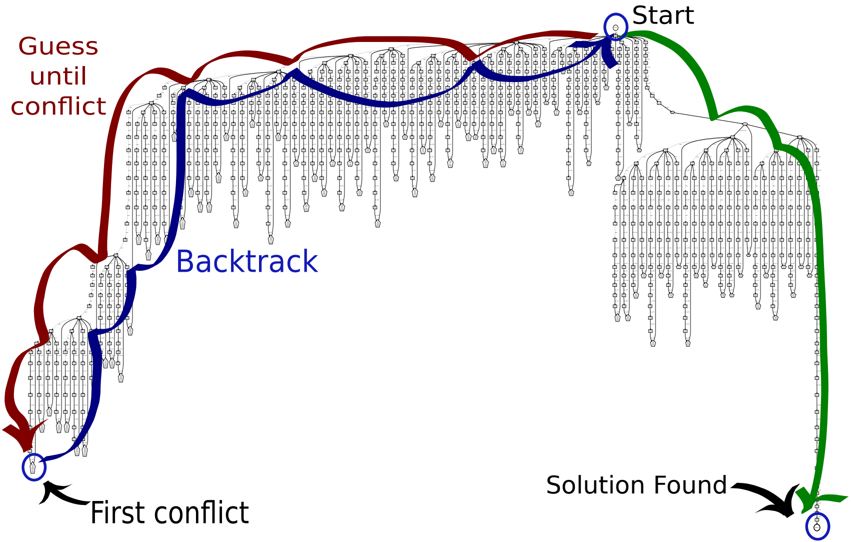
1. If (formula φ trivial) return SAT/UNSAT
2. ret $\leftarrow$ DPLL(φ with $v \leftarrow$ `true`)
3. If (ret = SAT) return SAT
4. ret $\leftarrow$ DPLL(φ with $v \leftarrow$ `false`)
5. If (ret = SAT) return SAT
6. return UNSAT

Toy Example

$$\underbrace{(\neg x_1 \vee \neg x_2 \vee x_3)}_{\text{Clause 1}} \quad \wedge \quad \underbrace{(\neg x_1 \vee x_2)}_{\text{Clause 2}} \quad \wedge \quad \underbrace{(\neg x_1 \vee \neg x_2)}_{\text{Clause 3}}$$

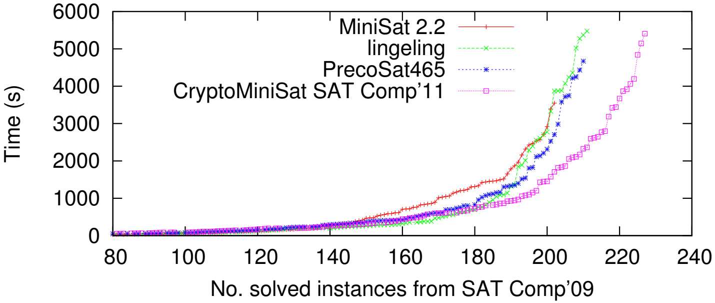
1. Guess: x_1 = True
2. Clause 2: x_2 = True
3. Clause 3: impossible! Reverse guess.
4. x_1 = False
5. Good, everything is satisfied!

Example Search Tree



CryptoMiniSat

- SAT solver that excels at cryptography
- General purpose: won SAT Race'10



- Collaborative: GPL, mailing list, regular releases

Demo

1. Generate HiTag2 problem: Grain-of-Salt tool
2. Solve it using CryptoMiniSat
3. Analyse results: $\approx$ 2 days to break

Conclusion

- SAT solvers are powerful tools to break weak cryptography
- CryptoMiniSat, a leading SAT solver, is waiting for your contribution
- Weak ciphers like HiTag2 should not be used in high-value applications