Cryptanalysis of the Cellular Message Encryption Algorithm

David Wagner
University of California, Berkeley
daw@cs.berkeley.edu

Bruce Schneier
Counterpane Systems
schneier@counterpane.com

John Kelsey
Counterpane Systems
kelsey@counterpane.com

Organization

- Intro to cellphone crypto and CMEA
- Cryptanalysis of CMEA
- Impact and conclusions

Introduction

The history of North American cellphone security measures:

- '74 AT&T designs original security model; scanners non-existent
- '83 Analog cellphones (AMPS) widely available
- 80's Scanners, fraud become serious problem
- '86 Legislation: eavesdropping banned
- '92 More legislation: manufacture, import of cellular scanners banned
- '92 Digital cellphone standard (IS-54)
  - Standard includes crypto for first time
- '95 Crypto found in all digital cellphone standards

Introduction

Scale:

- ~50 million cellphone users
- By 2001, ~20 million digital cellphone users
- Millions of (analog) scanners; widely available for ~$300
- ~$500 million/year lost to fraud (MIN/ESN cloning)

Legislation has failed; fraud and privacy violations are rampant.
Crypto is the only solution.

Introduction

Overview of cellphone crypto:

- ↑ CAVE: mixing function for authentication and key generation (anti-fraud)
- ↓ xor mask: voice privacy
- ↓ ORYX: LSFR-based stream cipher (wireless data)
- ↓ CMEA: block cipher for the control channel

Introduction

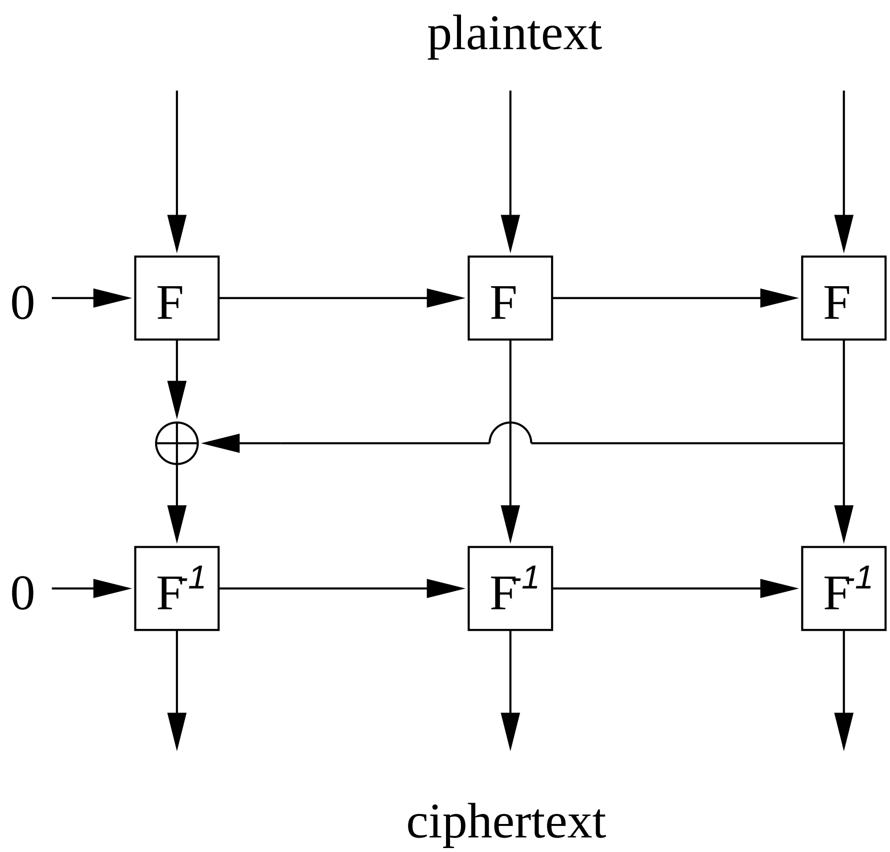
CMEA used to protect:

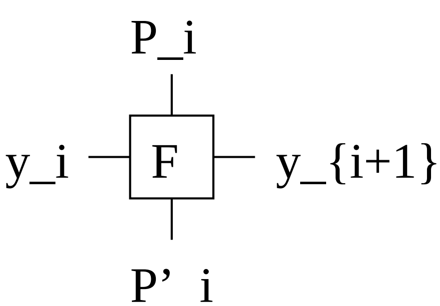
- Control channel messages
- Digits dialed on keypad (telephone numbers, calling card and voicemail PINs, ...)
- Alphanumeric pages

Our contribution:

CMEA has serious security flaws.

CMEA





$$P'_i = P_i + T(y_i \oplus i)$$

$$y_{i+1} = y_i + P'_i$$

$$T(x) = C(((C(((C(((C((x \oplus K_0) + K_1) + x) \oplus K_2) + K_3) + x) \oplus K_4) + K_5) + x) \oplus K_6) + K_7) + x$$

C a 8-bit-to-8-bit S-box (reused from CAVE)

Cryptanalysis

Known-plaintext attack on CMEA with 3-byte blocks:

- Crucial foot in the door: bias in C leads to exploitable bias in the T-box
- Phase 1: recover partial information about T-box, using known texts
- Phase 2: intelligent search for K, using info on T-box
- Complexity: 2^{24}–2^{32} work, 40–80 known texts, minutes–hours on a laptop

Phase 1

To recover partial information about the (keyed) T-box:

- Because of bias in C, 92 out of 256 possible values for $T(i)$ can be ruled out a priori
- Guess $T(0)$
- Gradually eliminate possible values for $T(i)$ using known texts
  - Find implications of the form $T(i) = j \Rightarrow T(k) = l$
  - Use contrapositive

Phase 2

To recover K using partial info about T:

- Pruned search
  - Work backwards (guessing $K_8, K_7, \ldots$) from known T-box outputs
  - Bias in C makes some intermediate results impossible
  - Disadvantage: exponential work if not enough info on T-box
- Meet-in-the-middle
  - Precompute table of size 2^{24}; do 2^{32} work
  - Faster than pruned search, but requires 4 fully-known T-box entries
- For best results, combine both

Cryptanalysis

Summary of attacks:

- Chosen-plaintext: 340 texts; mostly impractical
- Known-plaintext:
  - 3-byte blocks: $2^{24} - 2^{32}$ work, 40–80 texts; applies to all NA digital systems
  - 2-byte blocks: $2^{29} - 2^{37}$ work, 4 texts; CDMA only

In short, CMEA is seriously flawed.

Impact

Impact of CMEA cryptanalysis:

- Digits dialed, alphanumeric pages exposed
- Exploitable by anyone with digital scanner and strong technical skills

The state of cellphone security:

- Privacy protection (voice, digits) seriously flawed
- Fraud protection remains unbroken
- Digital cellphones still somewhat more secure than analog (CDMA somewhat more than TDMA), but long term forecast seems bleak

Conclusions

- Serious flaws in CMEA;
  widespread attacks may be practical
- Need open design process; proprietary algorithms are too dangerous
- Reuse of security components is risky:
  - Reused CAVE's S-box in CMEA because memory was short, but CMEA requires different properties than CAVE does
- Don't underestimate the power of economics and politics to re-shape your security model:
  - NSA/FBI pressured industry to cripple privacy protections
  - Industry's main interest was in stopping $500 mil/year losses to fraud

Acknowledgement

Greg Rose first pointed out the insecurity of CMEA, and he deserves the credit for that discovery.

We were not aware of serious flaws in CMEA until we heard over the grapevine that he had found an effective known-plaintext attack on CMEA; this tip provided the motivation to look more closely at CMEA until we managed to independently re-derive the attack described in this paper. Unfortunately he is not free to publish his analysis, so we offer ours instead. We are extremely grateful to Greg Rose for his immeasurable help.