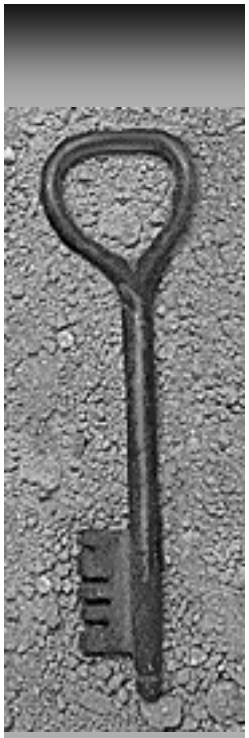
Cellphone Security

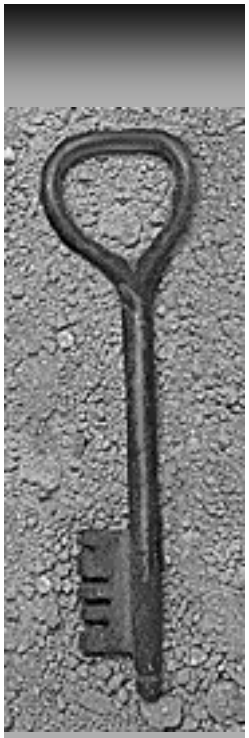
David Wagner
U.C. Berkeley



Cellular Systems Overview

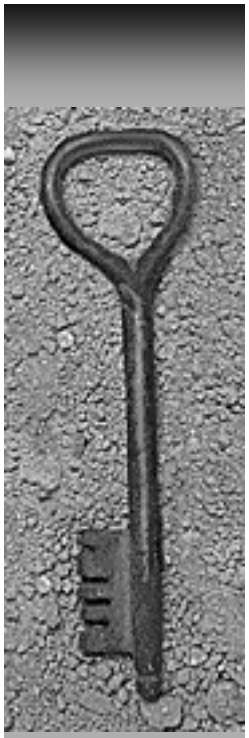
- Cellphone standards from around the world:

North America	Analog	AMPS
	Digital	CDMA, TDMA, N-AMPS
Europe	Digital	GSM



Cellular Crypto Algorithms

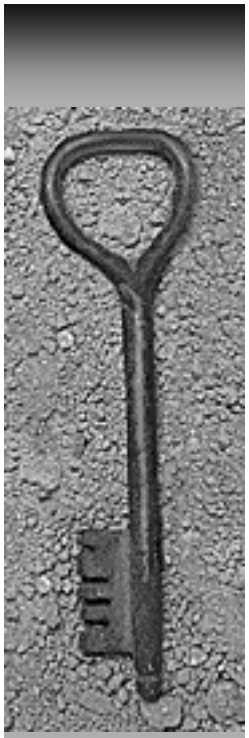
	Confidentiality	Authentication	Keying
US Analog	None	None	None
US Digital	XOR mask & CMEA (ORYX)	CAVE	CAVE
GSM	A5/0, A5/2, or A5/1 (soon: A5/3)	COMP128 (COMP128-2, 3DES-CBC-MAC)	COMP128 (same)



Cellular Crypto Algorithms

	Confidentiality	Authentication	Keying
US Analog	~~None~~	~~None~~	~~None~~
US Digital	~~XOR mask~~ & CMEA (ORYX)	CAVE	CAVE
GSM	~~A5/0,~~ A5/2, or A5/1 (soon: A5/3)	COMP128 (COMP128-2, 3DES-CBC-MAC)	COMP128 (same)

Key: ~~X~~ = insecure

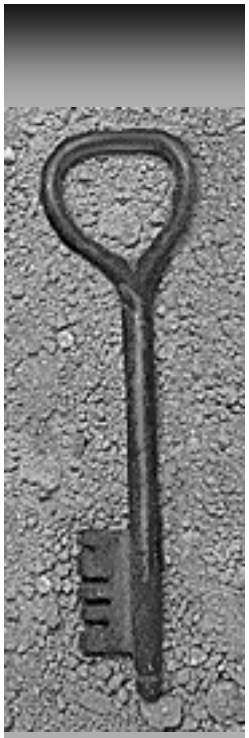


Cellular Crypto Algorithms

	Confidentiality	Authentication	Keying
US Analog	~~None~~	~~None~~	~~None~~
US Digital	~~XOR mask~~ & ~~CMEA (ORYX)~~	CAVE	CAVE
GSM	~~A5/0, A5/2,~~ or ~~A5/1~~ (soon: A5/3)	~~COMP128~~ (COMP128-2, 3DES-CBC-MAC)	~~COMP128~~ (same)

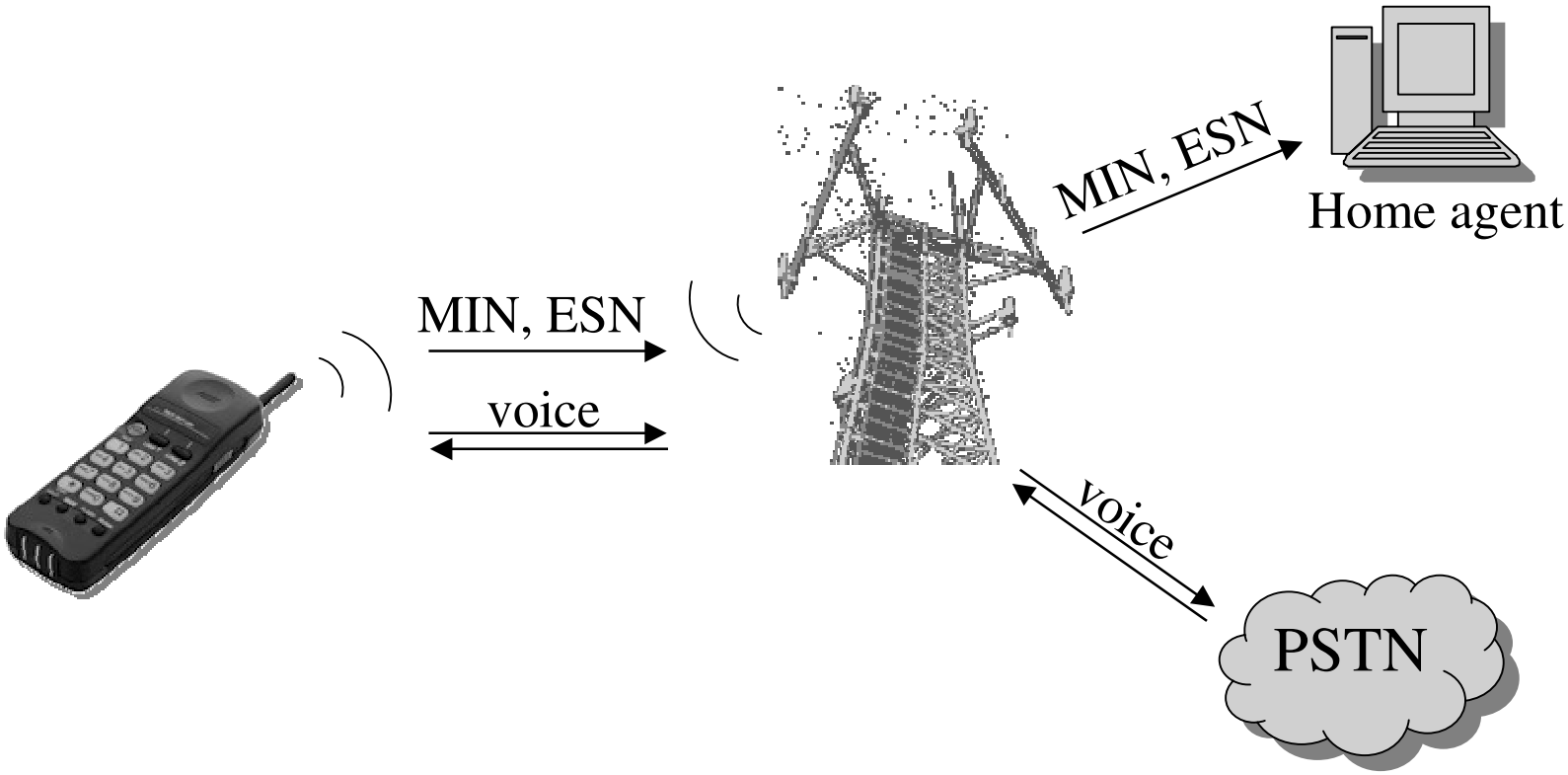
Key: ~~ ~~ = insecure

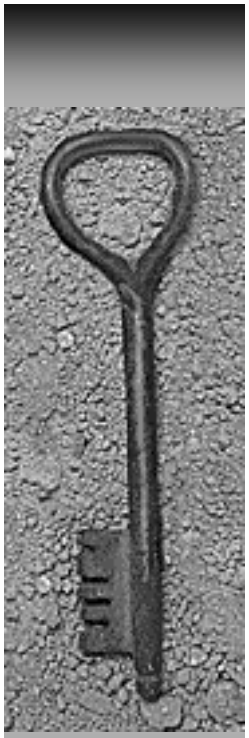
Part I:
North American Analog Systems



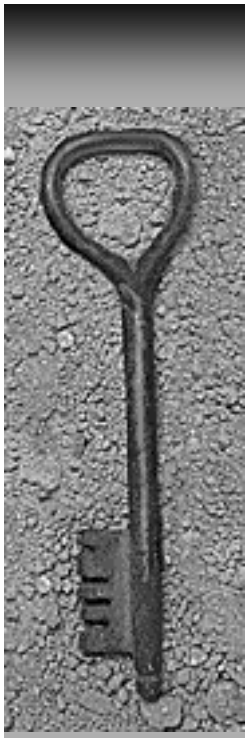
Overview of US Analog Protocol

- Everything goes in the clear:



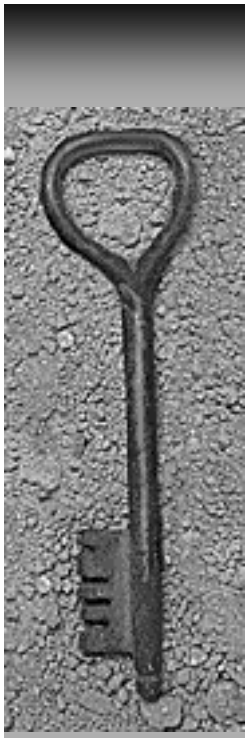


Vulnerabilities: Early Frauds



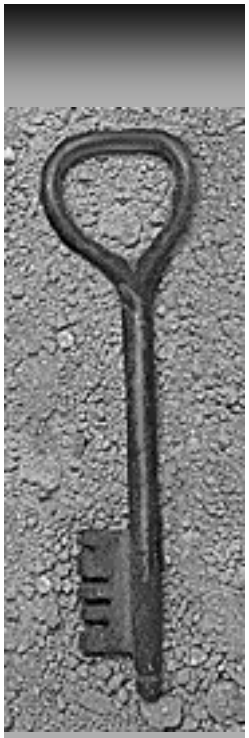
Vulnerabilities: Early Frauds

- At first, billing was done offline when roaming



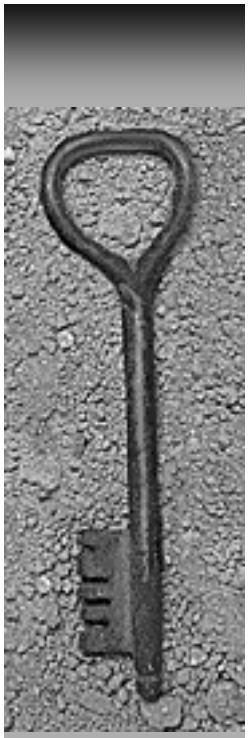
Vulnerabilities: Early Frauds

- At first, billing was done offline when roaming
  - Then criminals discovered one could pick a random MIN/ESN pair and make free calls



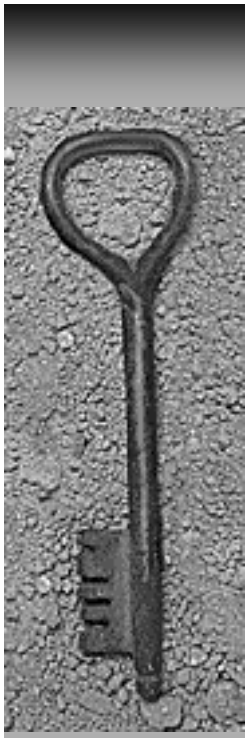
Vulnerabilities: Early Frauds

- At first, billing was done offline when roaming
  - Then criminals discovered one could pick a random MIN/ESN pair and make free calls
- So, providers added blacklists to base stations



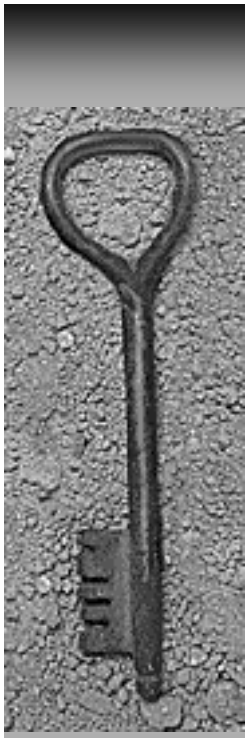
Vulnerabilities: Early Frauds

- At first, billing was done offline when roaming
  - Then criminals discovered one could pick a random MIN/ESN pair and make free calls
- So, providers added blacklists to base stations
  - But the first use of any MIN/ESN pair was unauthenticated, so criminals made very long calls



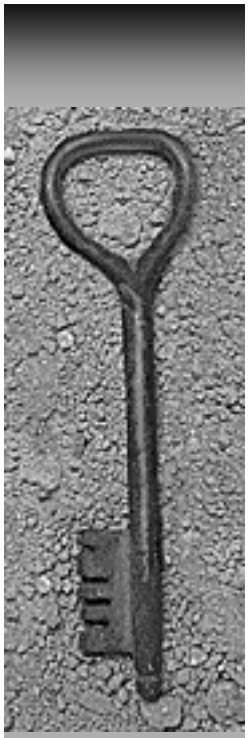
Vulnerabilities: Early Frauds

- At first, billing was done offline when roaming
  - Then criminals discovered one could pick a random MIN/ESN pair and make free calls
- So, providers added blacklists to base stations
  - But the first use of any MIN/ESN pair was unauthenticated, so criminals made very long calls
  - Later, *tumbling*: use a new MIN/ESN pair each time



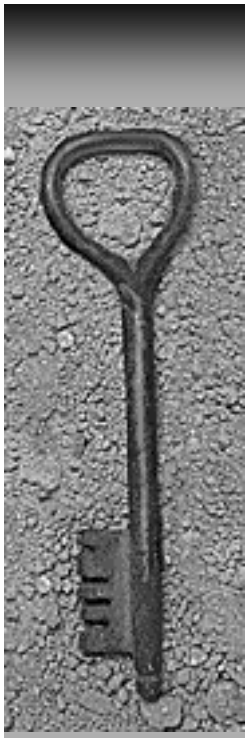
Vulnerabilities: Early Frauds

- At first, billing was done offline when roaming
  - Then criminals discovered one could pick a random MIN/ESN pair and make free calls
- So, providers added blacklists to base stations
  - But the first use of any MIN/ESN pair was unauthenticated, so criminals made very long calls
  - Later, *tumbling*: use a new MIN/ESN pair each time
- Countermeasure: realtime positive authentication



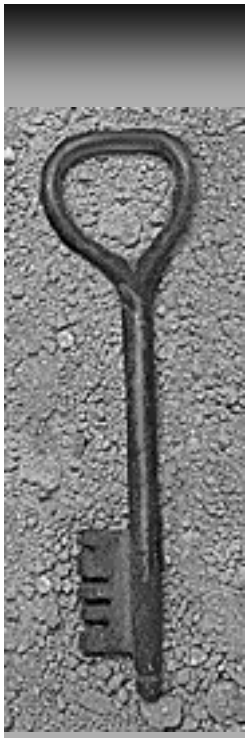
Vulnerabilities: Early Frauds

- At first, billing was done offline when roaming
  - Then criminals discovered one could pick a random MIN/ESN pair and make free calls
- So, providers added blacklists to base stations
  - But the first use of any MIN/ESN pair was unauthenticated, so criminals made very long calls
  - Later, *tumbling*: use a new MIN/ESN pair each time
- Countermeasure: realtime positive authentication
  - But *cloning* attacks became deadly: eavesdrop on MIN/ESN pair from a legitimate user, replay them later



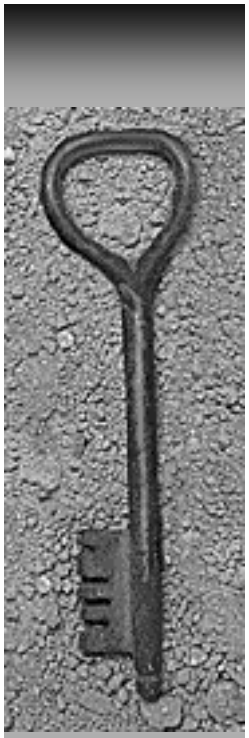
Vulnerabilities: Early Frauds

- At first, billing was done offline when roaming
  - Then criminals discovered one could pick a random MIN/ESN pair and make free calls
- So, providers added blacklists to base stations
  - But the first use of any MIN/ESN pair was unauthenticated, so criminals made very long calls
  - Later, *tumbling*: use a new MIN/ESN pair each time
- Countermeasure: realtime positive authentication
  - But *cloning* attacks became deadly: eavesdrop on MIN/ESN pair from a legitimate user, replay them later
  - Tumbling + cloning makes fraud hard to detect, black boxes widely available



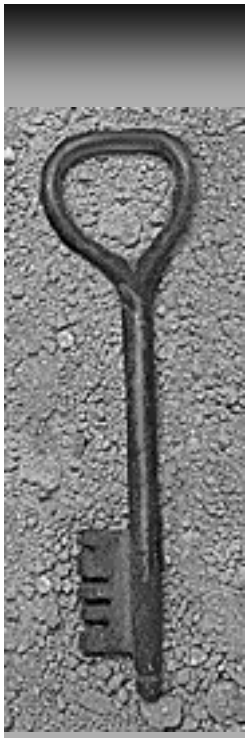
Impacts of Fraud

- Fraud a big problem in analog system
  - ≈ 5% of calls were fraudulent (~ 1995)
    (In Oakland on Friday night, reportedly 60-70%)
  - US losses: ≈ $650 million/year (≈ 2% of revenue)
- Attackers got organized & sophisticated
  - And early weaknesses gave criminals the capital and training to break future systems



Vulnerabilities: Privacy

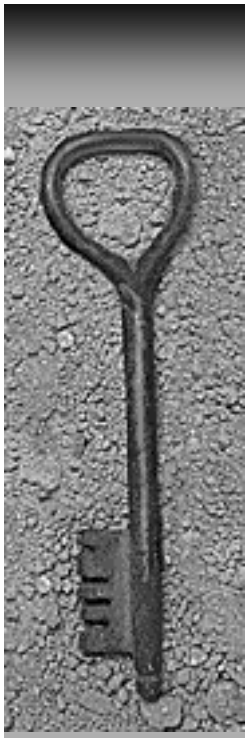
- Anyone can eavesdrop on voice calls
- Scanners (were) widely available
  - ≈10-15 million scanners sold on US mass market
  - ≈50 million users of US analog cellphones



Vulnerabilities: Privacy

- Anyone can eavesdrop on voice calls
- Scanners (were) widely available
  - ≈10-15 million scanners sold on US mass market
  - ≈50 million users of US analog cellphones

It seems plausible that the majority of US analog cellphone users may have had one of their calls intercepted at some point.

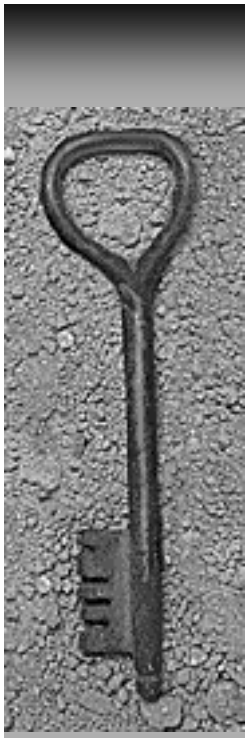


Summary on Analog Cellphones

- Everything that could go wrong, has
  - Threat models changed
  - Security architecture didn't scale up with deployment
  - We trained & funded a criminal underground

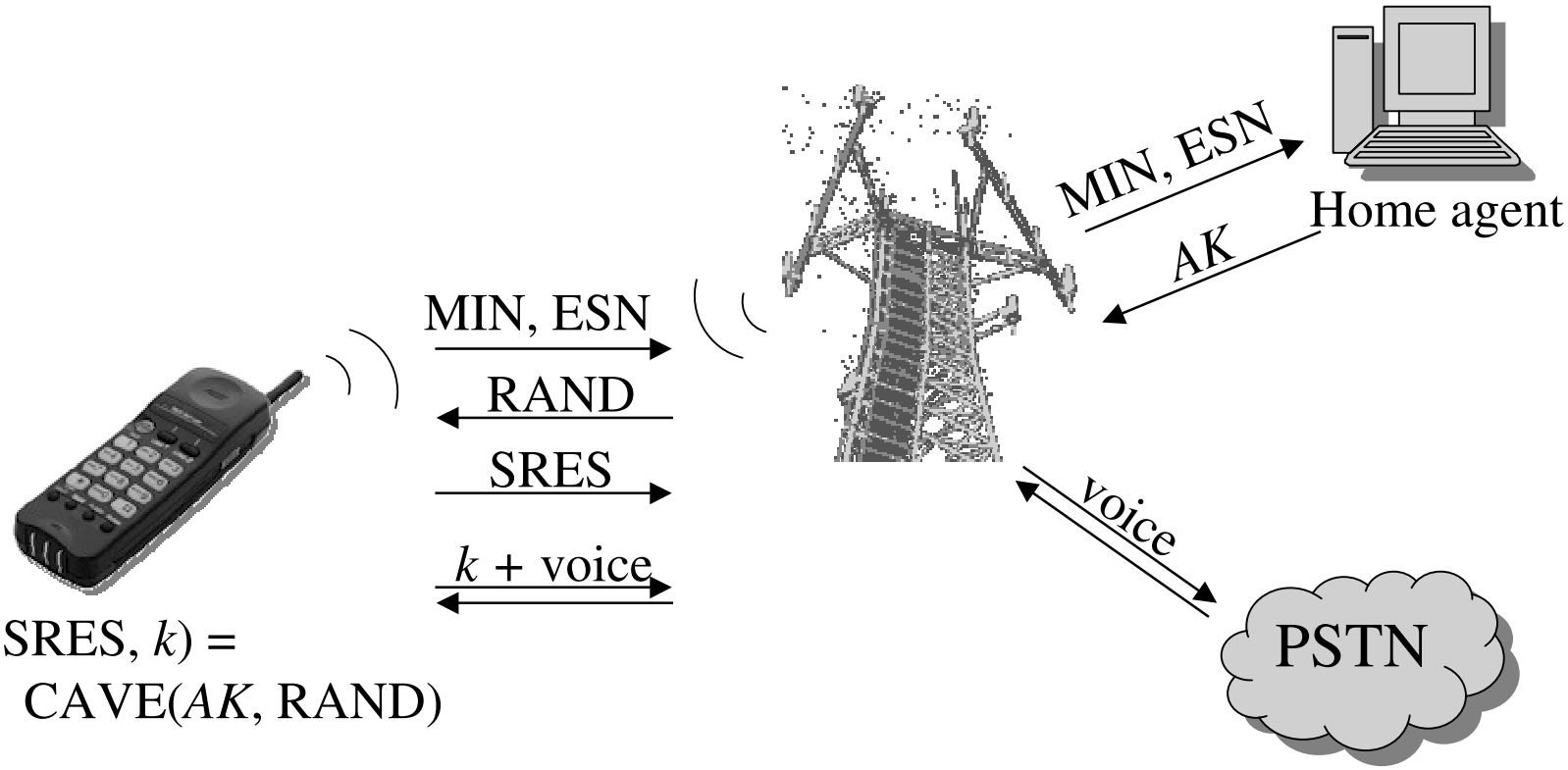
Analog cellphones are totally insecure.

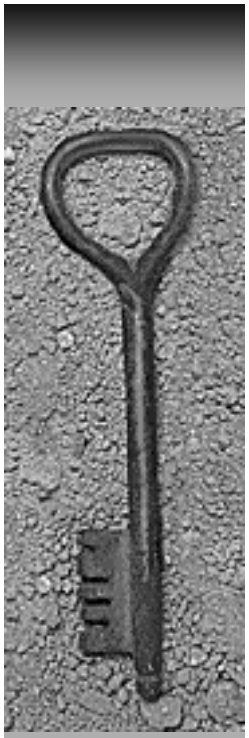
Part II
North American Digital Systems



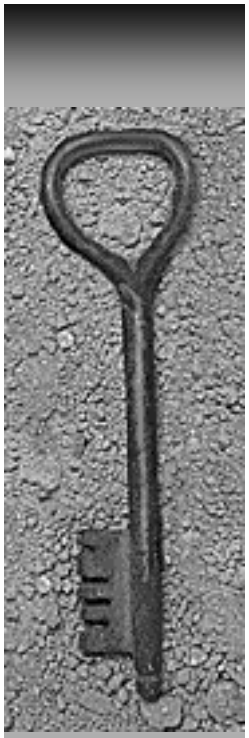
Overview of US Digital Protocol

- Crypto is used on the air link:



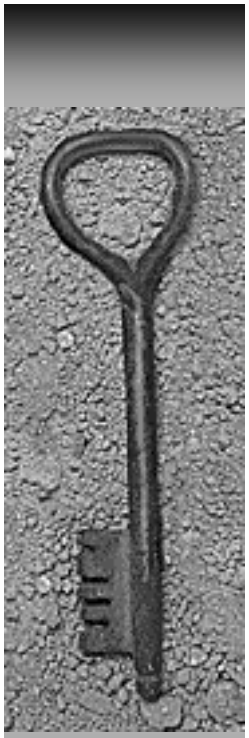


Cryptanalysis



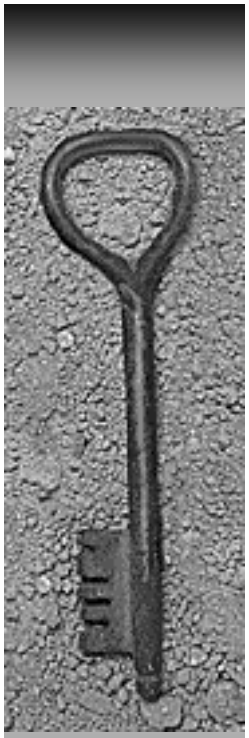
Cryptanalysis

- Voice privacy is XOR with 520-bit mask



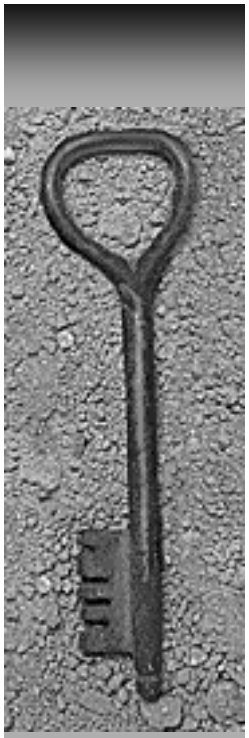
Cryptanalysis

- Voice privacy is XOR with 520-bit mask
  - Breakable in realtime via ciphertext-only attack [Bar92]; also, first frame is often silence (“all zeros”)



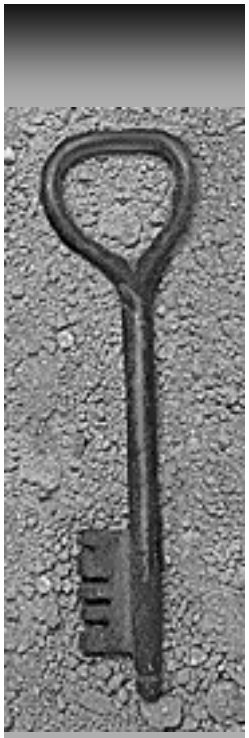
Cryptanalysis

- Voice privacy is XOR with 520-bit mask
  - Breakable in realtime via ciphertext-only attack [Bar92]; also, first frame is often silence (“all zeros”)
- Control channel uses CMEA, a variable-width block cipher with 2 rounds



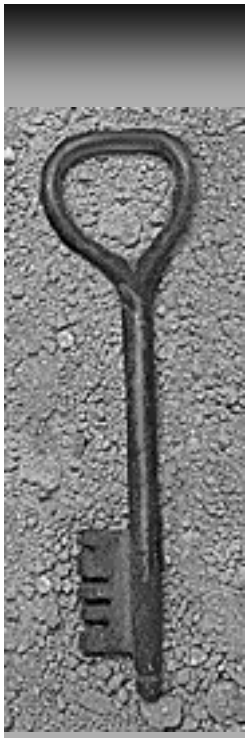
Cryptanalysis

- Voice privacy is XOR with 520-bit mask
  - Breakable in realtime via ciphertext-only attack [Bar92]; also, first frame is often silence (“all zeros”)
- Control channel uses CMEA, a variable-width block cipher with 2 rounds
  - Breakable in hours with 80 known texts [WSK97]



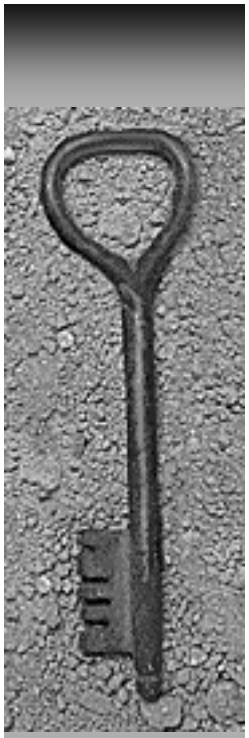
Cryptanalysis

- Voice privacy is XOR with 520-bit mask
  - Breakable in realtime via ciphertext-only attack [Bar92]; also, first frame is often silence (“all zeros”)
- Control channel uses CMEA, a variable-width block cipher with 2 rounds
  - Breakable in hours with 80 known texts [WSK97]
- ORYX, a LFSR-based stream cipher, was proposed for data traffic



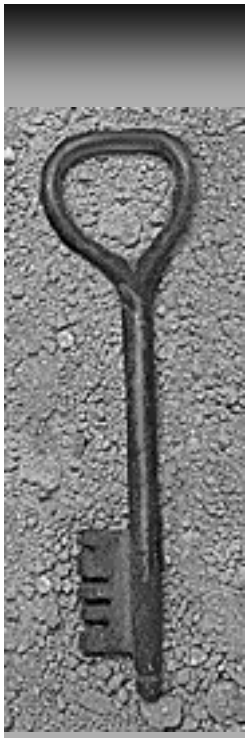
Cryptanalysis

- Voice privacy is XOR with 520-bit mask
  - Breakable in realtime via ciphertext-only attack [Bar92]; also, first frame is often silence (“all zeros”)
- Control channel uses CMEA, a variable-width block cipher with 2 rounds
  - Breakable in hours with 80 known texts [WSK97]
- ORYX, a LFSR-based stream cipher, was proposed for data traffic
  - Breakable in realtime via ciphertext-only attack [WSDKMS98]



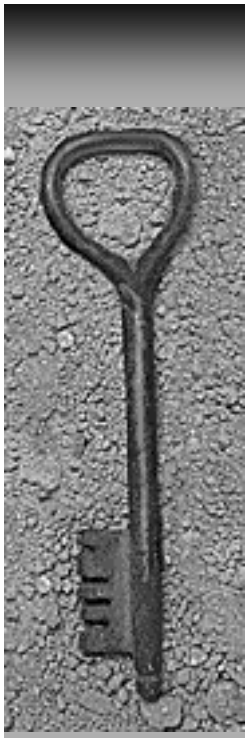
Cryptanalysis

- Voice privacy is XOR with 520-bit mask
  - Breakable in realtime via ciphertext-only attack [Bar92]; also, first frame is often silence (“all zeros”)
- Control channel uses CMEA, a variable-width block cipher with 2 rounds
  - Breakable in hours with 80 known texts [WSK97]
- ORYX, a LFSR-based stream cipher, was proposed for data traffic
  - Breakable in realtime via ciphertext-only attack [WSDKMS98]
- CAVE is a dedicated hash with 64-bit key



Cryptanalysis

- Voice privacy is XOR with 520-bit mask
  - Breakable in realtime via ciphertext-only attack [Bar92]; also, first frame is often silence ("all zeros")
- Control channel uses CMEA, a variable-width block cipher with 2 rounds
  - Breakable in hours with 80 known texts [WSK97]
- ORYX, a LFSR-based stream cipher, was proposed for data traffic
  - Breakable in realtime via ciphertext-only attack [WSDKMS98]
- CAVE is a dedicated hash with 64-bit key
  - Best attack I know needs 2^{21} chosen texts [Wag97]



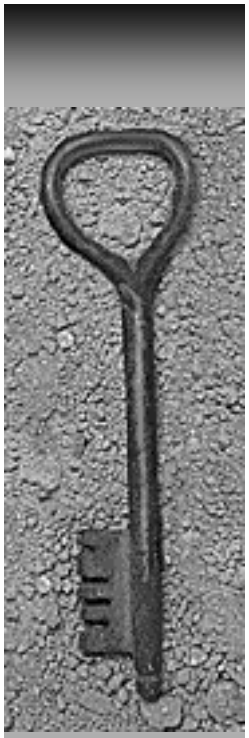
Why the Crypto May Not Matter

- Few base stations support encryption
  - It costs more
- Some handsets have $AK = 0$
  - Key management considered too expensive

Security of US digital cellphones rests primarily on cost of digital scanners and existence of easier targets.

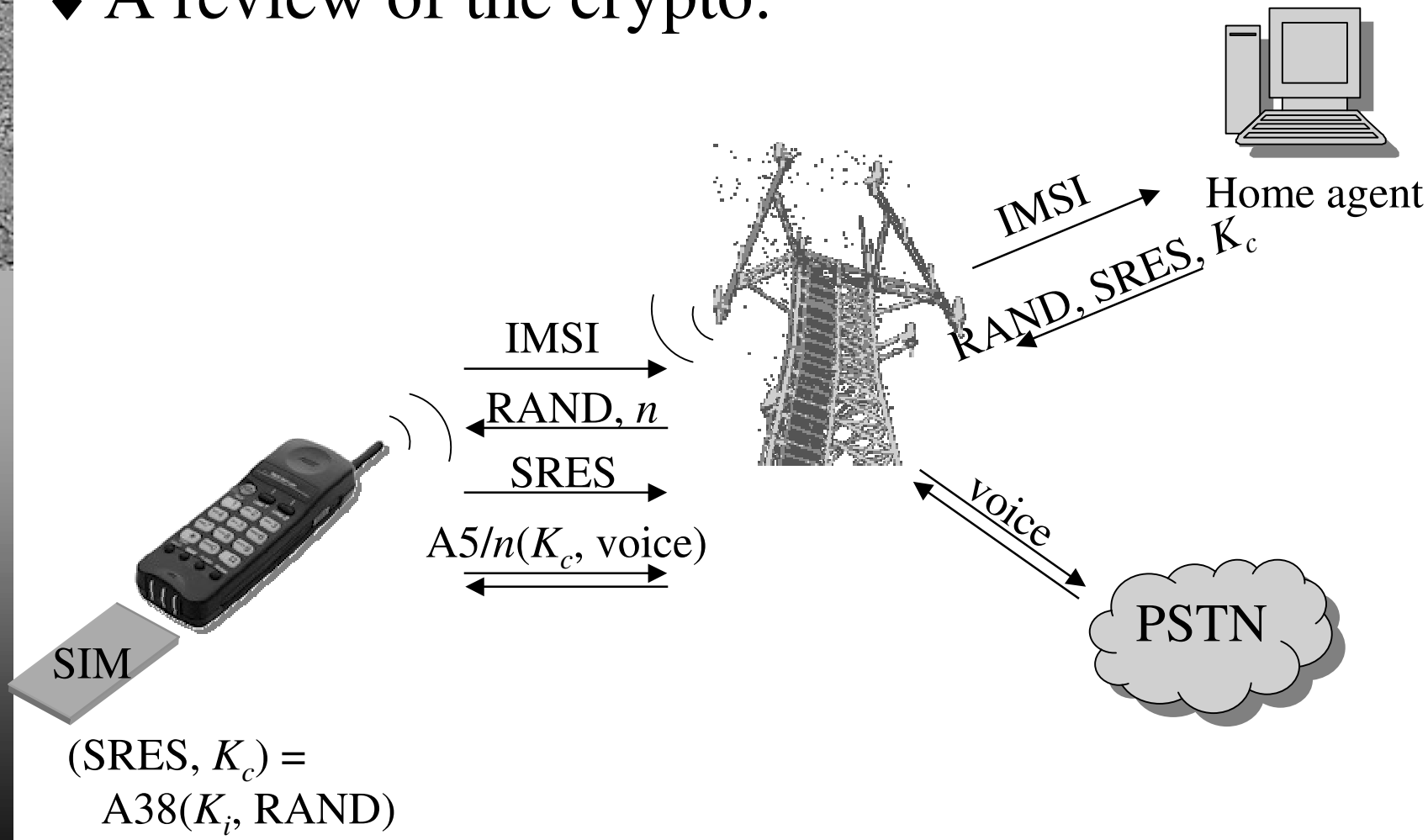
And many digital phones will fall back to analog, in areas of poor coverage.

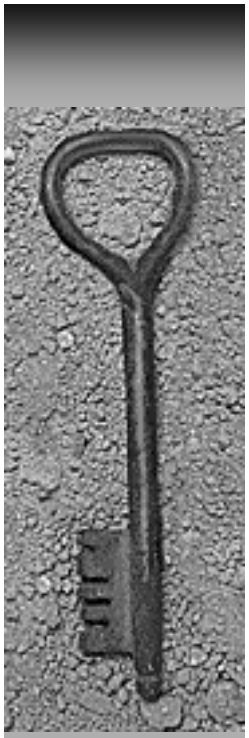
Part III
GSM



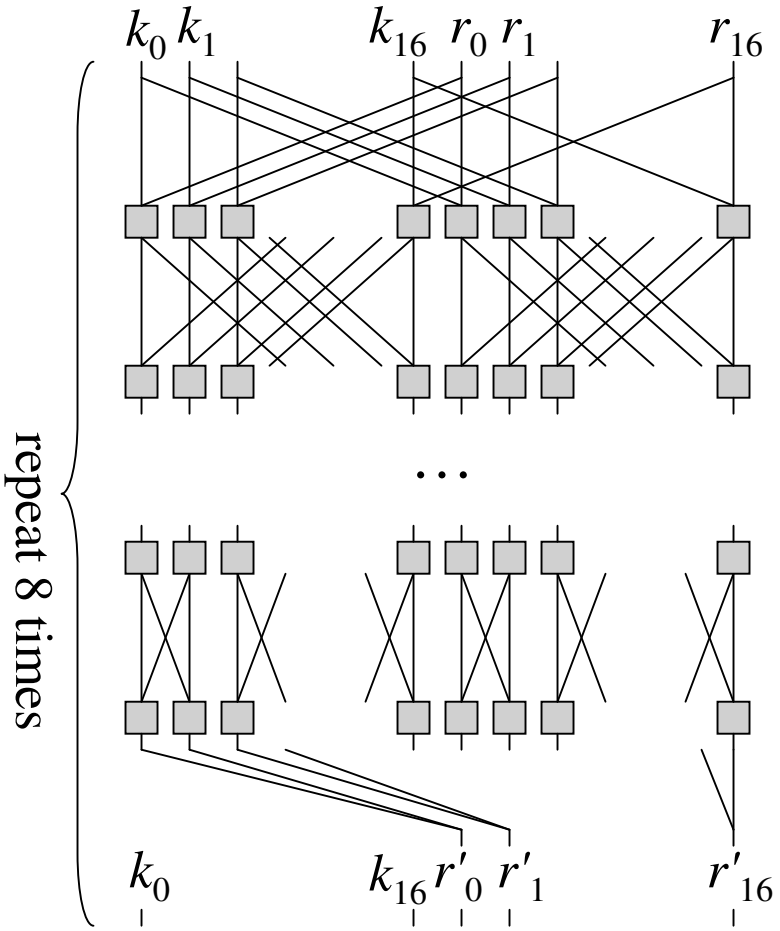
Overview of GSM Protocol

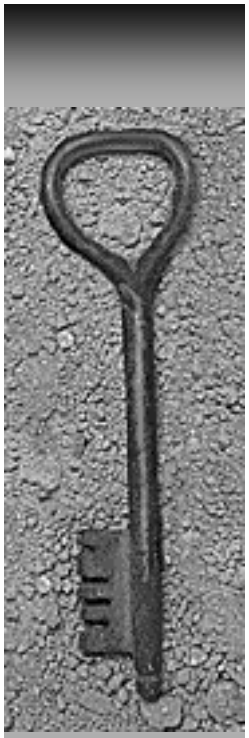
- A review of the crypto:





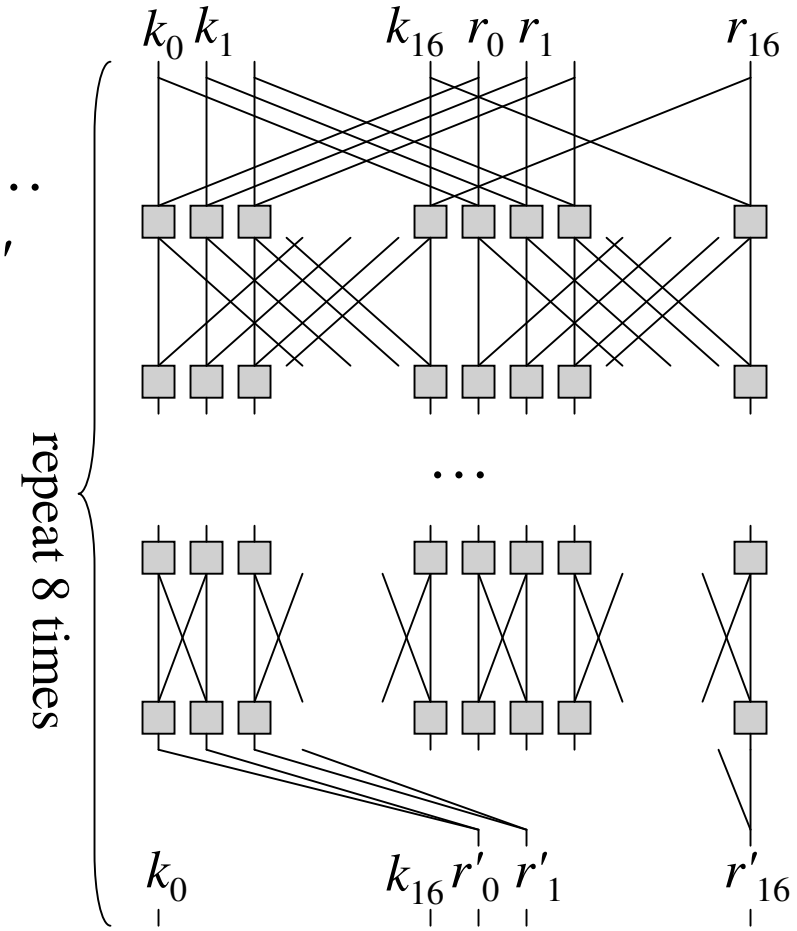
Cryptanalysis of COMP128

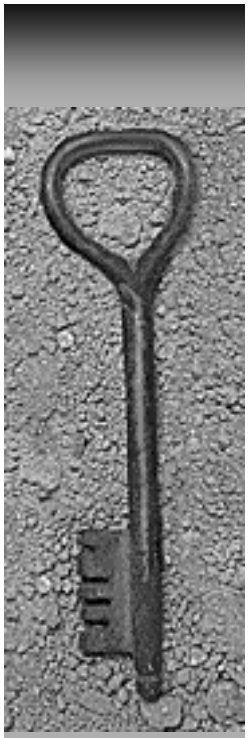




Cryptanalysis of COMP128

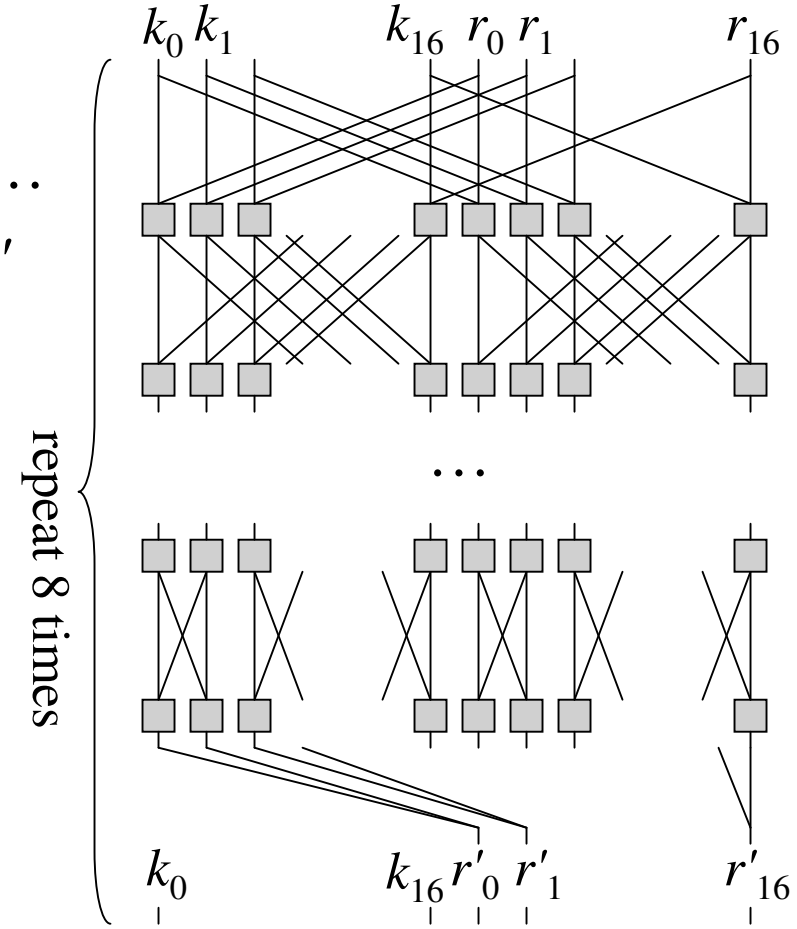
- Is it secure?
  - Well, it has lots of rounds…
  - The keyed map $f_k : r \mid\!\rightarrow r'$ is applied 8 times

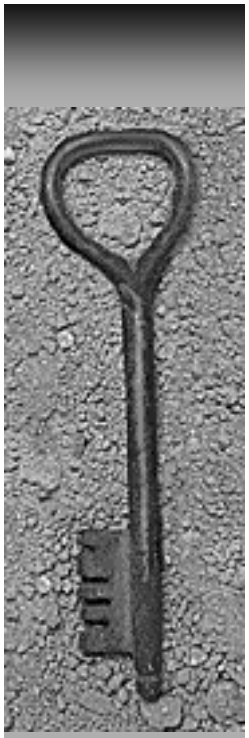




Cryptanalysis of COMP128

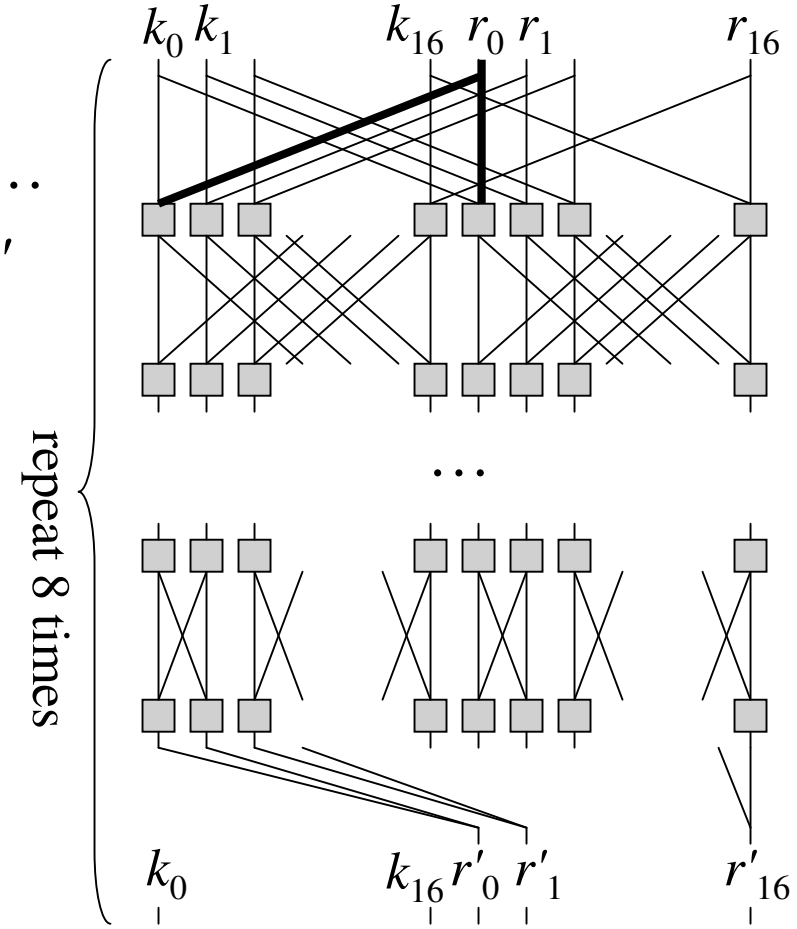
- Is it secure?
  - Well, it has lots of rounds…
  - The keyed map $f_k : r \mid\!\rightarrow r'$ is applied 8 times
- But: beware collisions!
  - Attempt #1: flip a bit in r_0 and hope for an internal collision

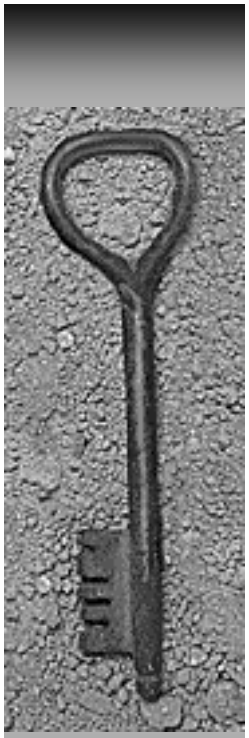




Cryptanalysis of COMP128

- Is it secure?
  - Well, it has lots of rounds…
  - The keyed map $f_k : r \mid\!\rightarrow r'$ is applied 8 times
- But: beware collisions!
  - Attempt #1: flip a bit in r_0 and hope for an internal collision

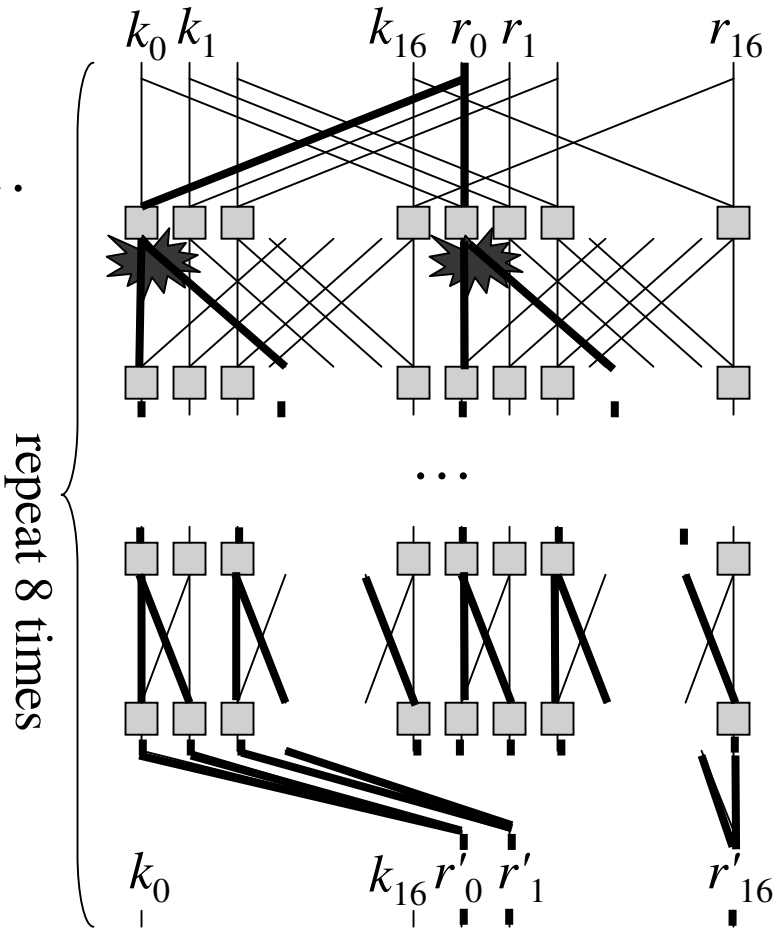


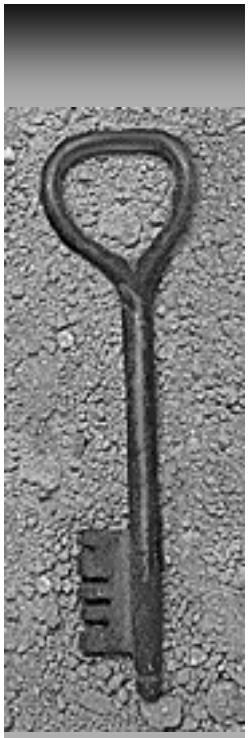


Cryptanalysis of COMP128

- Is it secure?
  - Well, it has lots of rounds…
  - The keyed map $f_k : r \mid\!\rightarrow r'$ is applied 8 times
- But: beware collisions!
  - Attempt #1: flip a bit in r_0 and hope for an internal collision

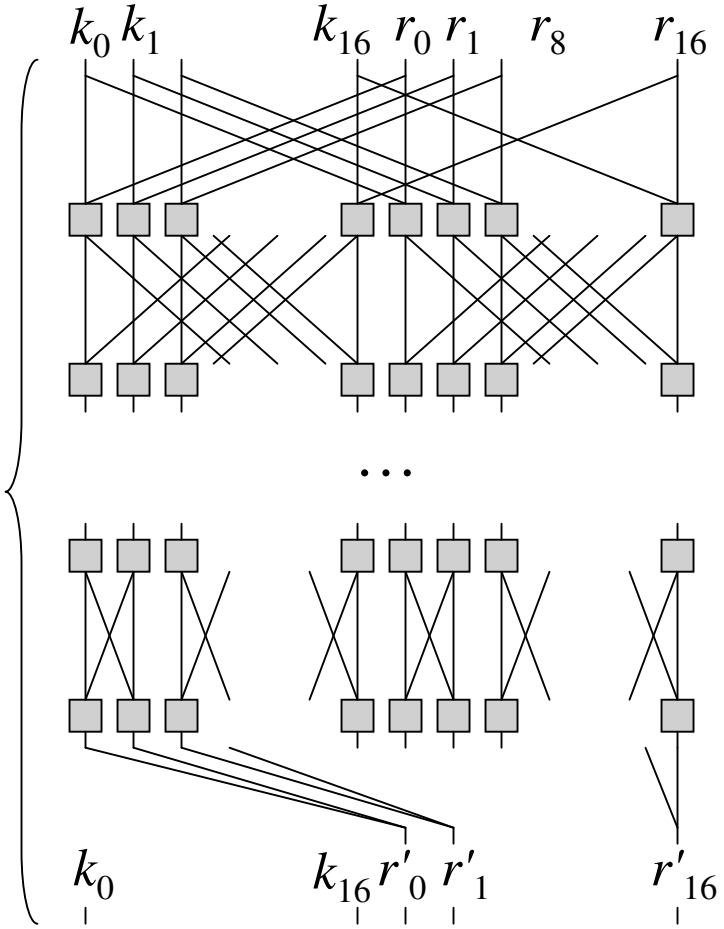
Doesn't work: such a collision can never happen

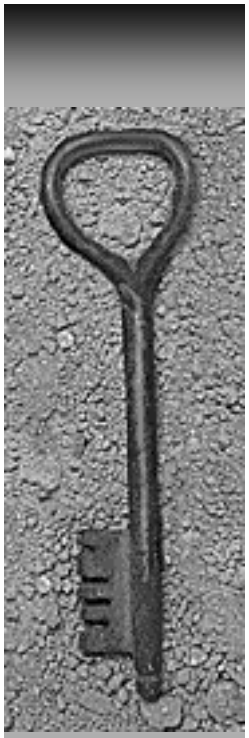




Cryptanalysis of COMP128

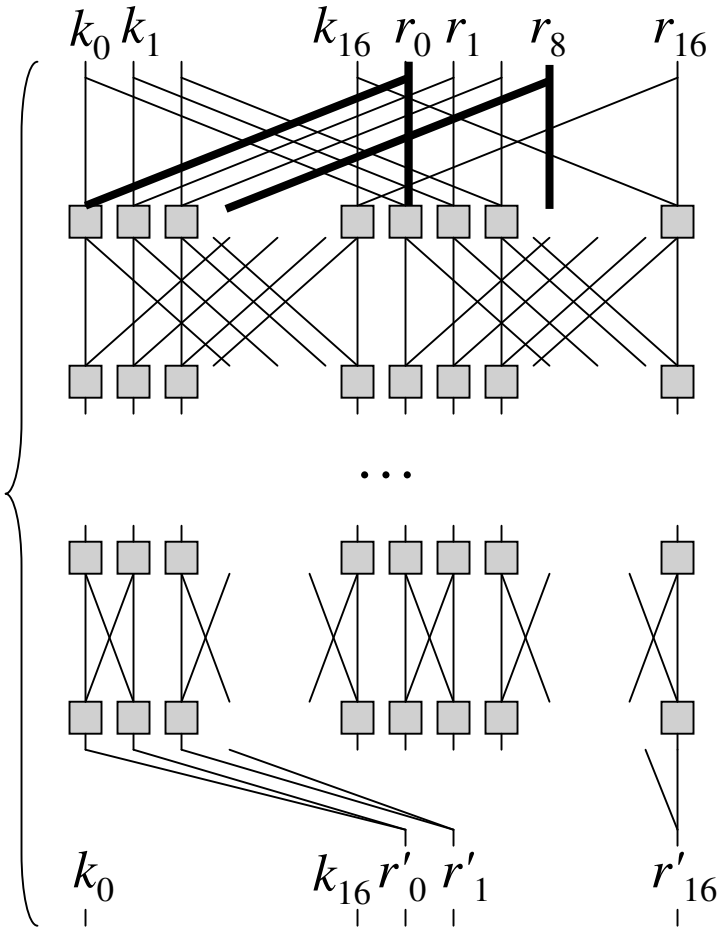
- Is it secure?
  - Well, it has lots of rounds…
  - The keyed map $f_k : r \mid\!\rightarrow r'$ is applied 8 times
- But: beware collisions!
  - Attempt #2: Modify both r_0 and r_8, and look for an internal collision [BGW98]

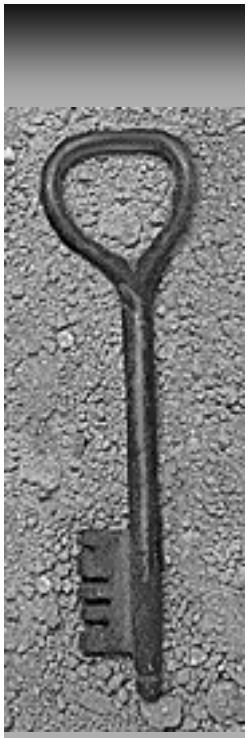




Cryptanalysis of COMP128

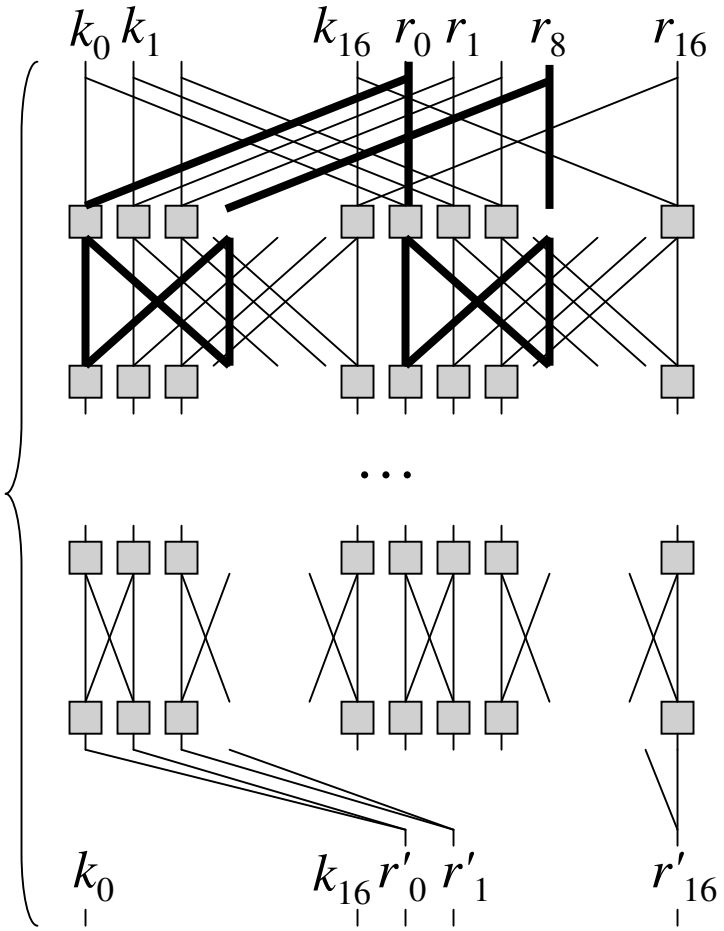
- Is it secure?
  - Well, it has lots of rounds…
  - The keyed map $f_k : r \mid\!\rightarrow r'$ is applied 8 times
- But: beware collisions!
  - Attempt #2: Modify both r_0 and r_8, and look for an internal collision [BGW98]

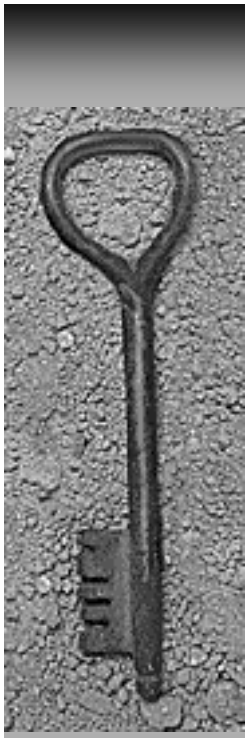




Cryptanalysis of COMP128

- Is it secure?
  - Well, it has lots of rounds…
  - The keyed map $f_k : r \mid\!\rightarrow r'$ is applied 8 times
- But: beware collisions!
  - Attempt #2: Modify both r_0 and r_8, and look for an internal collision [BGW98]

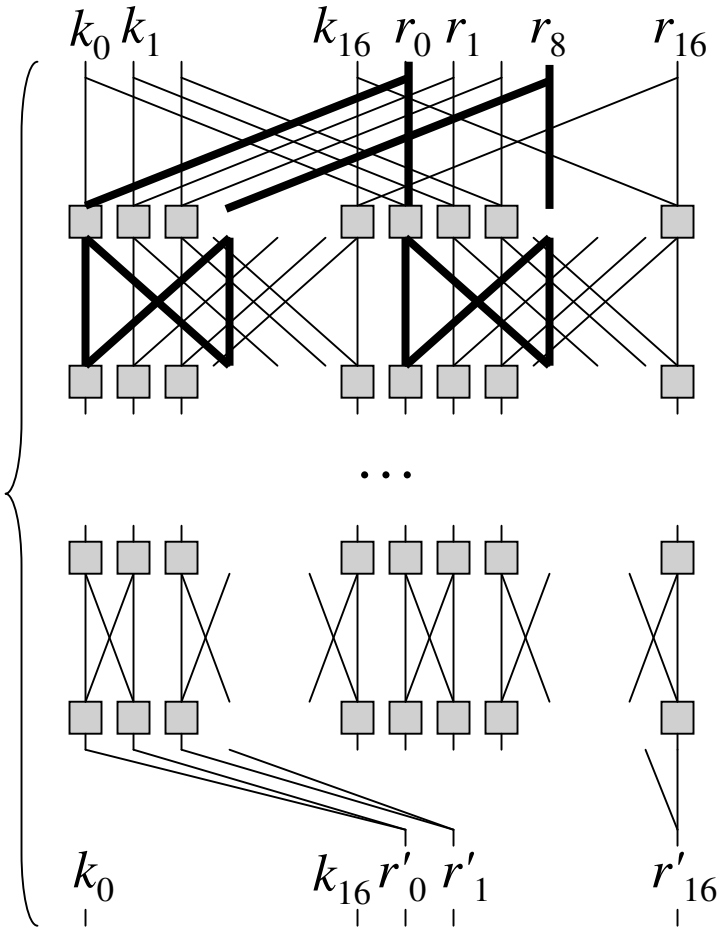


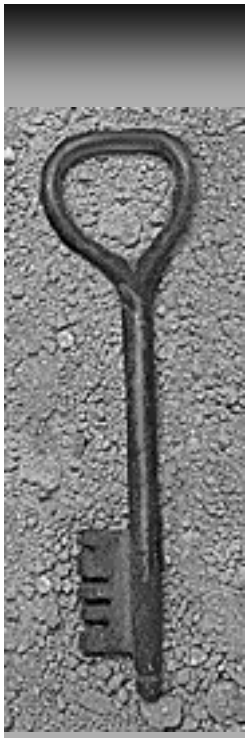


Cryptanalysis of COMP128

- Is it secure?
  - Well, it has lots of rounds…
  - The keyed map $f_k : r \mid\!\rightarrow r'$ is applied 8 times
- But: beware collisions!
  - Attempt #2: Modify both r_0 and r_8, and look for an internal collision [BGW98]

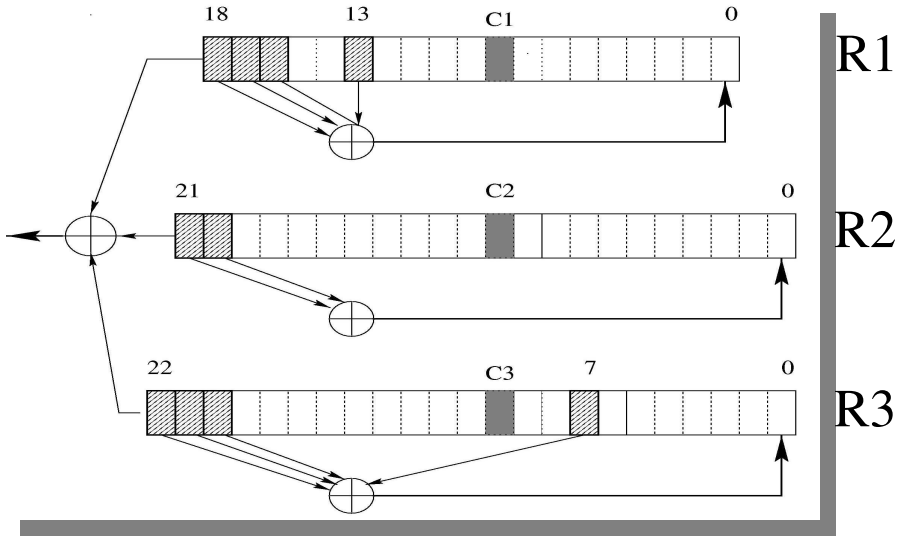
It works!



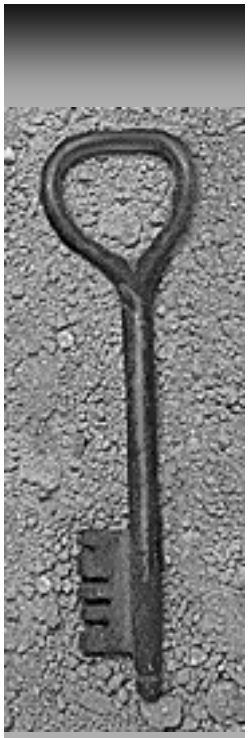


Cryptanalysis of A5/1

R*i* clocks just when
C*i* = Majority(C1,C2,C3)

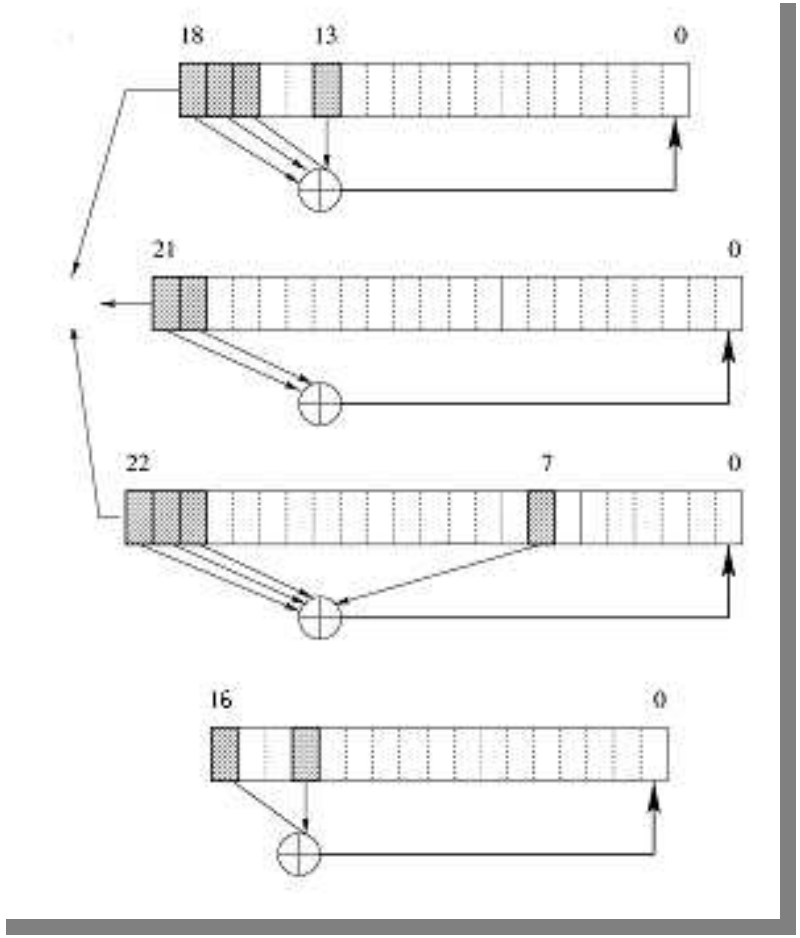


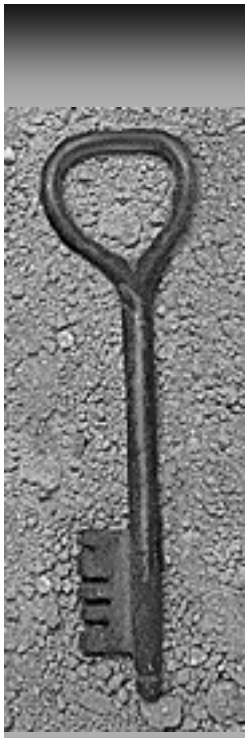
- Fix a 16-bit α; let S = $\{k : \mathrm{A5}(k) = \alpha \cdot \mathrm{any}\}$;
  define $f : \{0,1\}^{48} \rightarrow \mathrm{S}$ so that $f(x) = k$ with $\mathrm{A5}(k) = \alpha \cdot x$,
  noting that f can be computed efficiently;
  define $g : \{0,1\}^{48} \rightarrow \{0,1\}^{48}$ by $\alpha \cdot g(x) = \mathrm{A5}(f(x))$
- Apply Hellman's time-space tradeoff to g [BSW00]
  - Breaks A5/1 with 2^{24} work per key, 2^{36} space, & 2^{48} precomputation



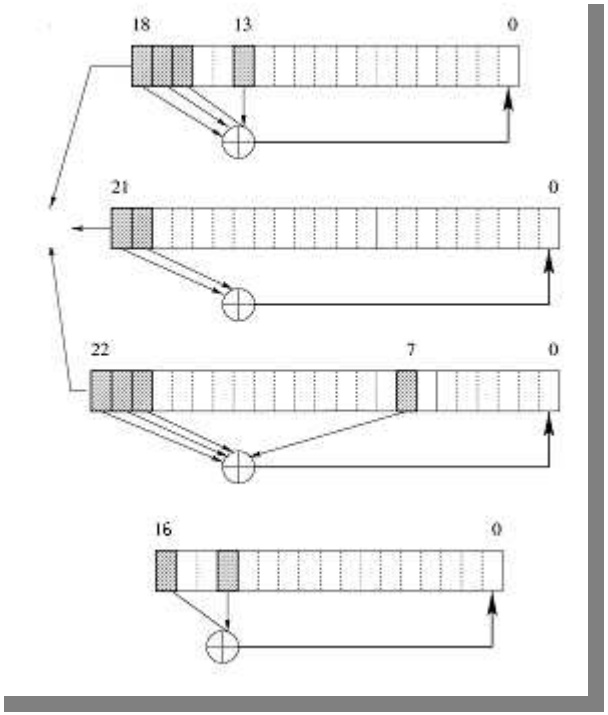
Description of A5/2

- Add a 17-bit LFSR, R4, that is clocked normally
- Clock control of R1, R2, R3 is a non-linear function of R4
- Output is quadratic function of R1, R2, R3
- After key loaded, one bit of each register is forced to be set (!!!)





One Evaluation of A5/2



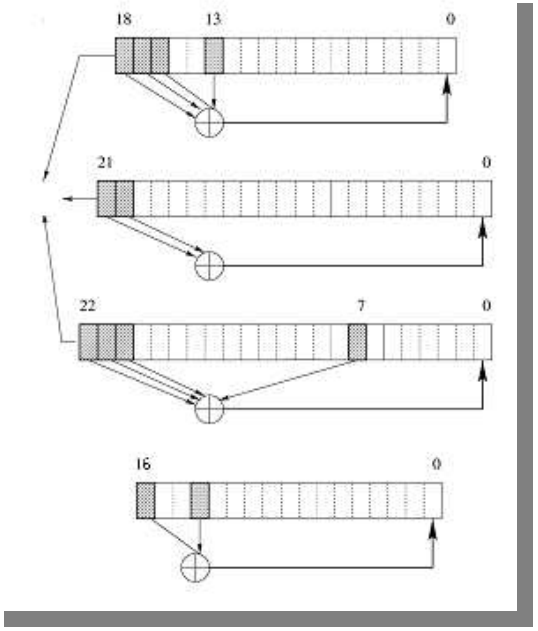
``The resource budget for the project was 15.75 man-months …

The results of the mathematical analysis did not identify any features of [A5/2] which could be exploited as the basis for a practical eavesdropping attack on the GSM radio path …

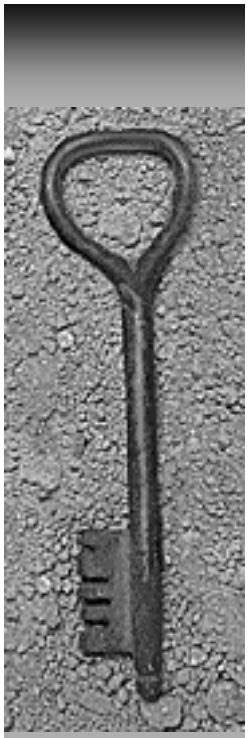
All members of SAGE stated that they were satisfied that [A5/2] was suitable to protect against eavesdropping on the GSM radio path''

-- ETSI TR 278

Attacking A5/2



- If you can get keystream from two frames 2^{11} apart:
  - R4 will be the same for both, due to the clobbered bit (hmm…)
  - Guess R4; then the clocking for R1, R2, R3 is known (double hmm…)
- Now solve for R1, R2, R3
  - Keystream difference is a linear function of R1, R2, R3 difference, so can solve using linear algebra
  - This reveals the key
- Complexity: 2^{16} simple dot-products $\Rightarrow$ realtime!
  - Our code breaks A5/2 in ~ 10 milliseconds [BGW99]



Concluding Thoughts

- Attacks are known on most of the cryptographic algorithms found in today's cellphones
- Questions?