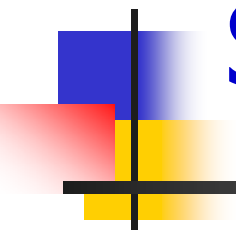


Stream Ciphers: Dead or Alive?

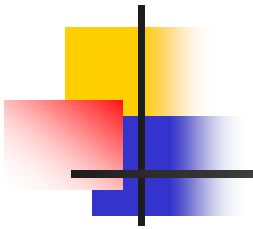
Adi Shamir
Computer Science Dept
The Weizmann Institute
Israel

ASIACRYPT 2004

At the RSA 2004 Cryptographers' Panel:

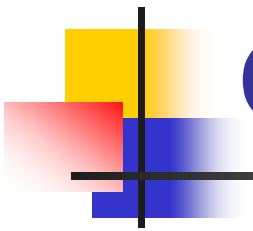
- I reviewed recent developments in cryptography
- I mentioned that stream ciphers are in trouble
- I predicted their death as a long term trend
- I was almost lynched as a result…

In this talk I would like to:



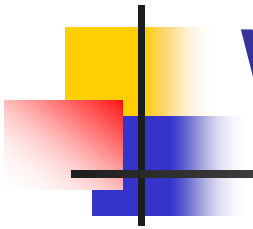
- Explain the past:
  - Why they were popular in the past
  - Why they became an endangered species
- Review the present:
  - What kind of stream ciphers are being proposed
- Predict the future:
  - Review promising new research directions
  - List some action items for our community

The Standard classification of Cryptosystems:



- Secret key algorithms
  - stream ciphers
  - block ciphers
- Public key algorithms
  - …

What is a stream cipher?



- The general idea is quite clear
- However, some schemes do not fall neatly into one of the two categories
- I tried to find precise definitions in some standard sources

What is a stream cipher?

- Menezes et al. Handbook of Applied Cryptography:

  Stream ciphers encrypt individual characters (usually binary digits) of a plaintext one at a time, using an encryption transformation which varies with time. By contrast, block ciphers tend to simultaneously encrypt groups of characters of a plaintext message using a fixed encryption transformation.

What is a stream cipher?

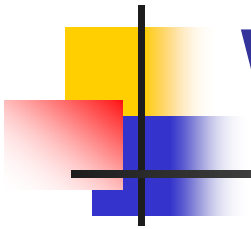
- R. Rueppel survey on stream ciphers:

  Block ciphers operate with a fixed transformation on large blocks of plaintext data; stream ciphers operate with a time-varying transformation on individual plaintext digits.

What is a stream cipher?

- RSA Labs FAQ:

While block ciphers operate on large blocks of data, stream ciphers typically operate on smaller units of plaintext, usually bits. The encryption of any particular plaintext with a block cipher will result in the same ciphertext when the same key is used. With a stream cipher, the transformation of these smaller plaintext units will vary, depending on when they are encountered during the encryption process.

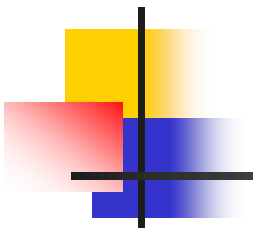


What is a stream cipher?

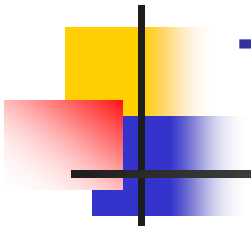
- Mentioned: the small plaintext size and transformation variability
- Ignored: The separation between key processing and plaintext processing, and the simplicity of the plaintext processing

- In fact, pure block and stream ciphers are two concrete points on a continuous design space, and we increasingly use mixed modes

The Decline of Stream Ciphers:



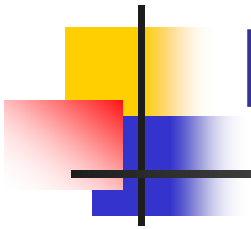
- Is a clear trend over the last 30 years
- Is driven by basic technological changes
- Is unlikely to be reversed in the near future



The Best Evidence for the Crisis:

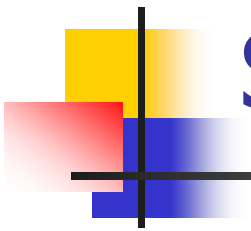
- I looked at the list of session names at ASIACRYPT 2004:
  - Block ciphers
  - Public key encryption
  - Number theory and algebra
  - Secure computation
  - Hash functions
  - Key management
  - Identification
  - XL-algorithms
  - Digital signatures
  - Public key cryptanalysis
  - Symmetric key cryptanalysis
  - Protocols

Possible Reasons to Prefer Block Ciphers Today:



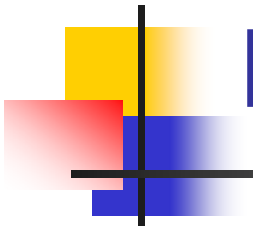
- Availability of standardized schemes
- More versatile building block
- Better understanding of security issues
- Better covered by textbooks and courses

Possible Reasons to Prefer Stream Ciphers today:



- A smaller footprint in low-end hardware implementations
- Higher encryption speed
- Smaller input/output delay
- Simpler protocols for handling small or variable sized inputs

However, They Are of Diminishing Importance:

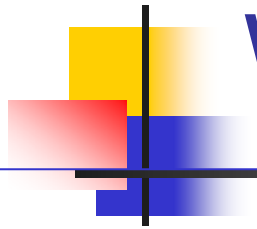


- Hardware gets larger AND cheaper
- More applications can be handled in software
- Encryption is typically not a speed bottleneck
- The input/output delay is usually insignificant
- Standardized packets make it unnecessary to handle small or variable sized inputs

I Believe That Stream Ciphers Will Become Niche Products:

- In large hardware implementations, speed is not a problem (block cipher counter mode can be easily parallelized to get arbitrarily high speed)
- In software implementations on a PC, footprint size is not a problem (program size and memory are plentiful)

I Believe That Stream Ciphers Will Become Niche Products:



- I believe that stream ciphers will remain competitive in two types of applications:
  - a hardware oriented scheme with exceptionally small footprint (gates, power consumption, etc)
  - a software oriented scheme with exceptionally high speed

Others Seem to Agree:

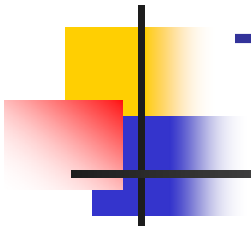
- The State of the Art in Stream Ciphers (SASC) workshop was held in October 2004 in Belgium
- Steve Babbage from Vodafone presented a paper:
  Stream Ciphers – What Does the Industry Want?
- His main conclusion:

  "stream ciphers are useful for:

  - Very high speed: multigigabit per second communication links (e.g., routers)
  - Efficient/compact in constrained devices (e.g., RFID's)"

Types of Security Applications:

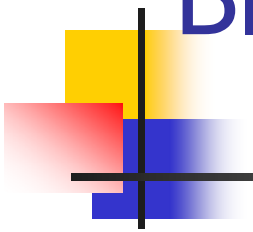
- Data storage: block oriented
- Data transmission: stream oriented, but:
  - Until the early 20-th century: messages written on paper were also block oriented
  - From the late 20-th century: computer, internet, satellite, VOIP use packets which are block oriented
  - There was a short period in the middle of the 20-th century when transmissions were stream oriented, using Morse or teletype codes



The Early Years of Cryptography

- Until the 1920's, essentially all the deployed cryptosystems were based on paper and pencil techniques, replacing and shuffling letters
- Schemes based on letter substitutions (with multiple alphabets) looked like stream ciphers
- Schemes based on letter permutations (moving them around a grid) looked like block ciphers
- Since most schemes used combinations of the two techniques to get reasonable security they should be classified as block ciphers.

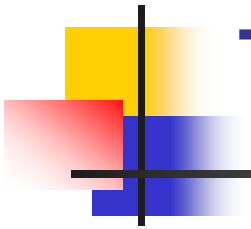
Block Ciphers Were Preferred Since:



- They were more general
- They were stronger
- Memory was cheap and plentiful (paper)
- Both stored and transmitted messages (letters) were in a form of a block of data, which was available all at once.

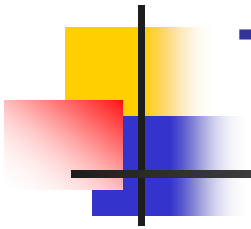
The 1920's revolution

- Radio was introduced, revolutionizing long range military and commercial mobile communication
- Transmitted data changed from parallel to serial
- The weakness of paper and pencil schemes was exposed in books such as "The Black Chamber"
- Rotor-based electromechanical encryption devices were developed and adopted all over the world
- Memory on these devices became very expensive: they could keep an internal state but not user data



The 1920's revolution

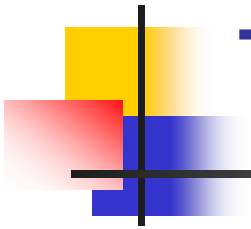
- This created a window of opportunity for stream ciphers, since input letters had to be dealt with serially during the encryption process
- The move to stream ciphers was supported by the development of the one time pad as the first theoretically unbreakable scheme



The Age of the Stream cipher

- Until the 1960's, everyone was using stream ciphers: Military and diplomatic services, spy organizations, telecommunication providers, major companies, etc.
- The schemes were either a one time pad, or a related scheme based on the electromechanical generation of pseudo randomness
- Mainframe computers were available, but were used more in cryptanalysis than in cryptography.

The Age of the Stream cipher

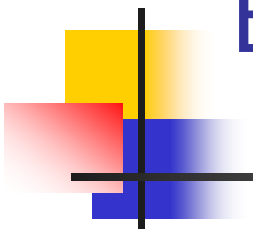


- In the 1960's, transistor-based electronic encryption devices started to appear
- The new devices also had very little memory, so stream ciphers continued to be much more popular than block ciphers
- A new design element was adopted: the linear feedback shift register
- It was supported by a well developed mathematical theory

The Emergence of the Modern Block Cipher in the late 20-th Century:

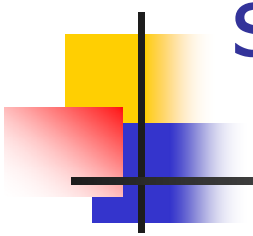
- Computers, satellites, telephony started to use block oriented packets
- VLSI-based electronic gates, memories and microprocessors started to appear, relaxing speed and circuit size constraints
- Block ciphers became easy to construct
- Military services continued to prefer stream ciphers, but new commercial applications demanded block ciphers

Some Implementors Switched to Block Ciphers at an Early Stage:



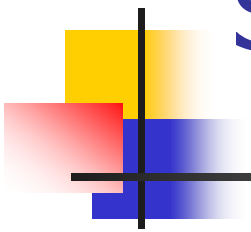
- Smart cards initially had very weak processors
- Hardware DES coprocessors were added
- Today's 16 and 32 bit smart card processors can easily handle any standard block cipher

Some Implementors are replacing stream cipher by block ciphers:



- Cellular telephony (GSM):
  - 2-nd generation: A5/x stream cipher
  - 3-rd generation: Kasumi block cipher
- Wireless networking (Wi-Fi):
  - 802.11a/b: RC4 stream cipher
  - 802.11i: AES block cipher

Some Holdouts:

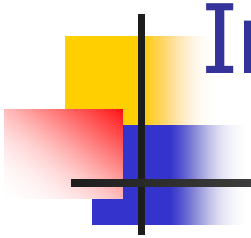


- Bluetooth: E0 stream cipher.
- Very limited footprint size and power consumption in bluetooth applications
- Development stopped by Ericsson

Some Future Applications:

- RFID's are extensively tested (in Korea and elsewhere).
- I believe it will be a very important and successful technology in the next decade
- The security aspects of RFID had not been standardized so far
- I expect them to use stream ciphers rather than block ciphers

Why Stream Ciphers Seem to be Inherently Weaker Than Block Ciphers



- Attacks on block ciphers (like differential attacks) are applicable also to stream ciphers
- Attacks on stream ciphers (like correlation attacks) are not applicable to block ciphers
- Algebraic attacks seem to be more useful against stream ciphers (especially LFSR based)

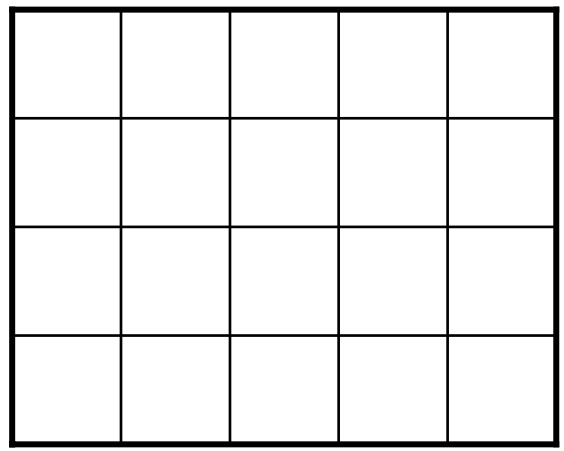
Why Stream Ciphers Seem to be Inherently Weaker Than Block Ciphers

- Guess and set attacks on stream ciphers can recover either the key or any state

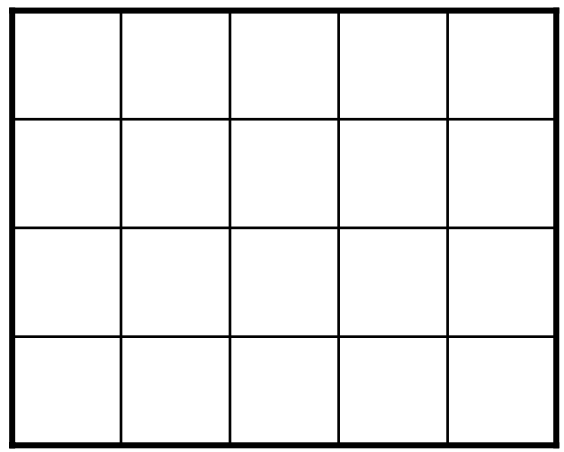
- Generic time/memory tradeoff attacks on stream ciphers ($TM^2D^2=N^2$) are stronger than the corresponding attacks on block ciphers ($TM^2=N^2$) since they can exploit the availability of a lot of data

Why Stream Ciphers Seem to be Inherently Weaker Than Block Ciphers

- Stream ciphers: time

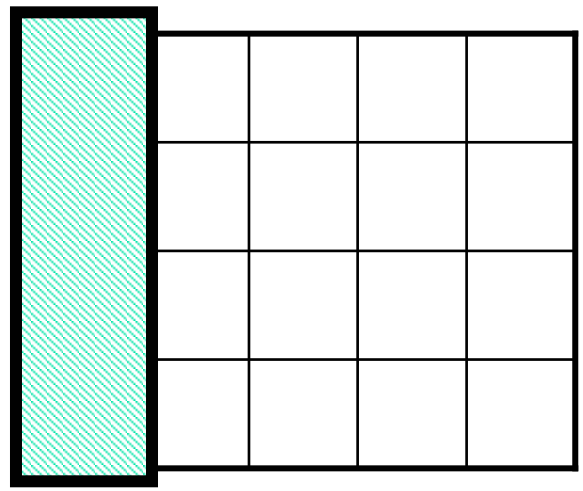


- Block ciphers: time

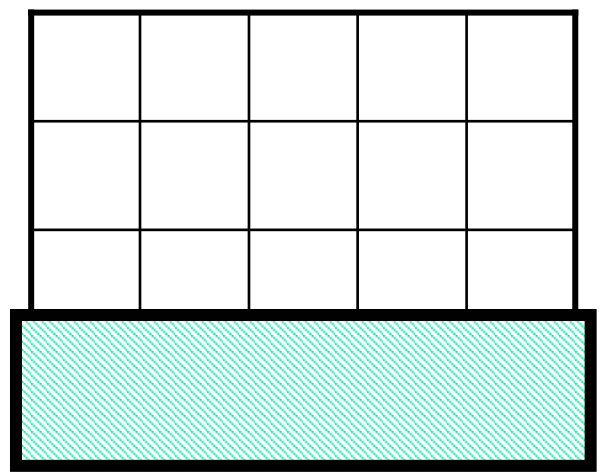


Why Stream Ciphers Seem to be Inherently Weaker Than Block Ciphers

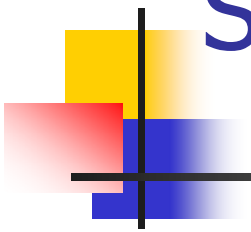
- Stream ciphers: time



- Block ciphers: time



Security Assessment of Ciphers:



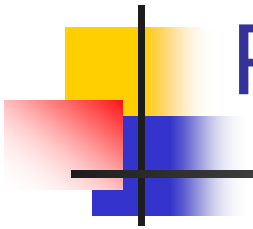
- Given a new block cipher, we have a good set of mature tools to assess its security
- Given a new stream cipher, its vulnerability is more likely to be one-of-a-kind
- Given a new public key cipher, it is likely to be insecure…

An Important Consideration: Can Governments Break Our Codes?

My personal unsubstantiated belief:

- In public key: academia is slightly ahead of governments
- In block ciphers: governments are slightly ahead of academia
- In stream ciphers: governments are way ahead of academia

Recent Trends in Stream Ciphers:



- Use 32/64 bit words as elements
- Use native microprocessor instructions
- Use elements from block ciphers
- Avoid linear structures
- Mix algebraic domains

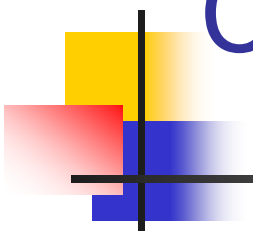
General Advice on the Design of New Stream Ciphers:

- Use simple minimal designs
- Study new primitives and generic attacks
- Design a two level key structure
- Avoid classical techniques which may be well studied by secret organizations
- Add rate reduction/security enhancement mechanisms into your design

The relative importance of Attacks:

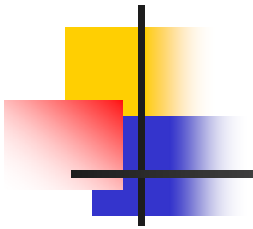
- Degree of linearity tests (??)
- Distinguishing attacks (?)
- Statistical tests
- Guess and set attacks
- Side channel attacks (!)
- Rekeying attacks (!)
- Correlation attacks (!!)
- Algebraic attacks (!!)

Other Types of Stream Ciphers:



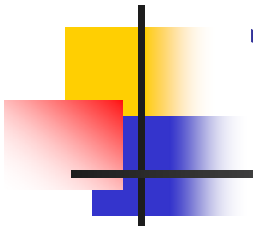
- Authenticated stream ciphers
- Self synchronizing stream ciphers

The Importance of Standards



- The standardization of DES in 1976 was a crucial precondition for the development of civilian applications of Cryptography
- The de-facto standardization of RSA made it well known and trusted
- The fact that no stream cipher is currently standardized is a huge burden on the field
- Soon: ISO standard for MUGI, SNOW 2

Summary



- I believe that stream ciphers are in an unavoidable long term decline
- I believe that stream ciphers will survive in some niche applications
- I believe that we urgently need some standard schemes of particular types
- I believe that our state of knowledge and level of confidence in stream ciphers is weak