# STRUCTURAL CRYPTANALYSIS OF SASAS

ALEX BIRYUKOV, ADI SHAMIR
APPLIED MATH DEPT
THE WEIZMANN INSTITUTE
ISRAEL



## STRUCTURAL CRYPTANALYSIS

- STUDIES WEAKNESSES ASSOCIATED WITH GENERAL BLOCK DIAGRAMS, RATHER THAN PARTICULAR CHOICE OF OPERATIONS
- APPLICABLE TO MANY CONCRETE SCHEMES
- HELPS DEVELOPE A GENERAL THEORY

EXAMPLES:

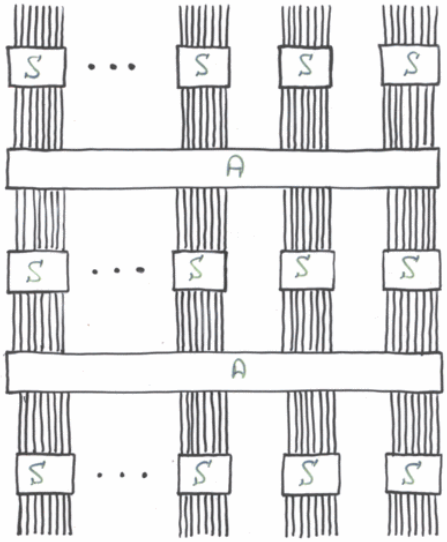
- FEISTEL STRUCTURES
- DOUBLE ENCRYPTION
- CHAINED MODES OF OPERATION



## WHAT IS THE SASAS SCHEME?

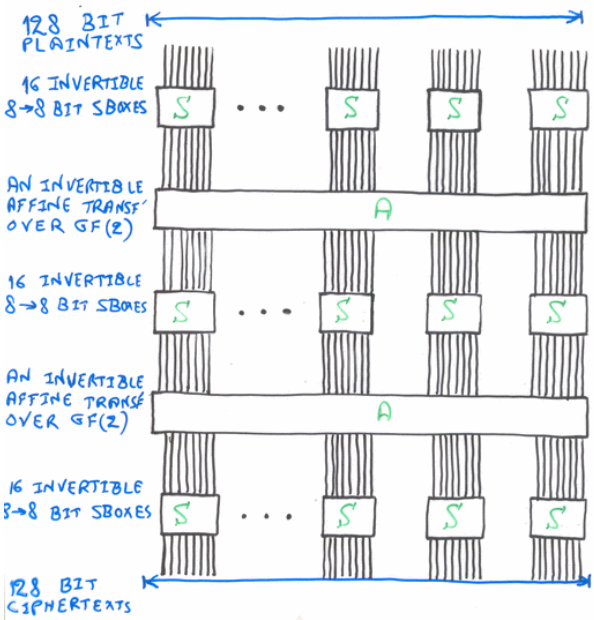
- SASAS IS **NOT** A CRYPTOSYSTEM WHICH WAS PROPOSED, STANDARDIZED, OR USED BY ANY PARTICULAR RESEARCHER
- SASAS COMBINES MANY DESIGN PRINCIPLES WHICH ARE BELIEVED TO LEAD TO STRONG CRYPTOSYSTEMS
- THE GOAL OF THE RESEARCH IS TO IDENTIFY THE EXACT NUMBER OF ITERATIONS WHICH SEPARATE WEAK AND STRONG VARIANTS

# THE STRUCTURE OF SASAS:






# THE STRUCTURE OF SASAS: TYPICAL SIZES:






# SASAS COMBINES STRONG INGREDIENTS

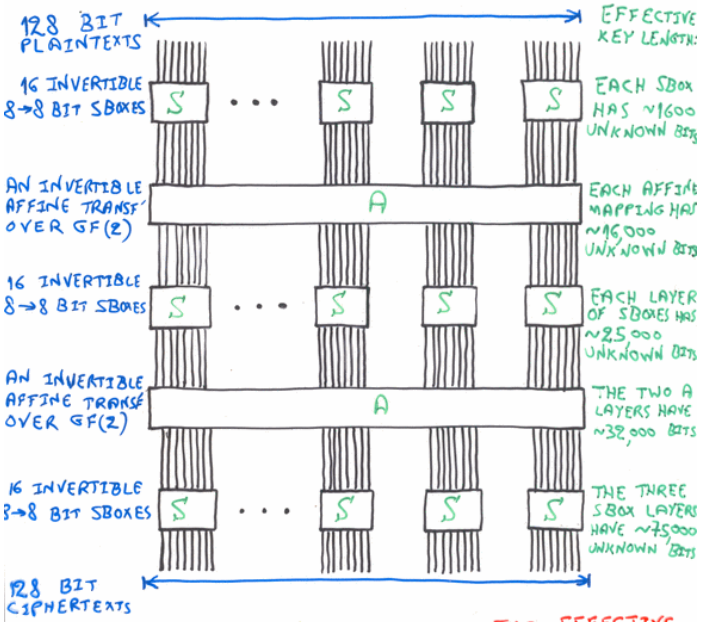
- USES SHANNON'S IDEA OF ALTERNATING CONFUSION/DIFFUSION LAYERS
- USES LARGE SBOXES WHICH ARE NOT LIKELY TO BE DEGENERATE
- USES DIFFERENT SBOXES AND AFFINE MAPPINGS AT THE VARIOUS LOCATIONS
- USES AFFINE MAPPINGS OVER BITS, RATHER THAN AFFINE MAPPINGS OVER BYTES OR PERMUTATIONS OVER BITS:

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{128} \end{bmatrix} = \begin{bmatrix} a_{1,1} & \cdots & a_{1,128} \\ \vdots & & \vdots \\ a_{128,1} & \cdots & a_{128,128} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{128} \end{bmatrix} + \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{128} \end{bmatrix} \pmod 2$$

- USES UNKNOWN AND KEY DEPENDENT SBOXES AND AFFINE MAPPINGS
- USES A HUGE EFFECTIVE KEY LENGTH



# THE STRUCTURE OF SASAS: TYPICAL SIZES:

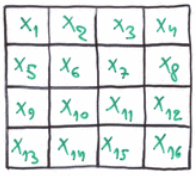



THE EFFECTIVE KEY LENGTH EXCEEDS 100,000 UNKNOWN BITS

8

## SIMILAR DESIGNS IN THE LITERATURE:

- MANY S-P NETWORKS (TYPICALLY WITH KNOWN S,P ELEMENTS, KEY XOR'ED TO INTERMEDIATE DATA, MORE ROUNDS)
- THE AES CANDIDATE RIJNDAEL:
  - A 4x4 ARRAY OF BYTES
  - A 10 ROUND CRYPTOSYSTEM WITH KNOWN OPERATIONS.




OPERATIONS:
- XOR A KEY TO EACH BYTE
- APPLY AN SBOX TO EACH BYTE
- ROTATE THE ROWS
- LINEARLY MIX THE COLUMNS

- PATARIN'S ALGEBRAIC 2R PUBLIC KEY CRYPTOSYSTEM: ASASA WHERE THE A'S ARE UNKNOWN LINEAR MAPPINGS AND THE S'S ARE UNKNOWN MULTIVARIATE QUADRATIC POLYNOMIALS. THE RESULTANT 4-DEGREE MULTIVARIATE POLYNOMIALS ARE PUBLIC KE

9

## PREVIOUSLY KNOWN ATTACKS:

THE SQUARE ATTACK ON RIJNDAEL

- USES THE FACT THAT THE PERMUTATION IS BYTE ORIENTED
- USES THE FACT THAT THE ROW ROTATIONS DISTRIBUTE A SINGLE COLUMN AMONG ALL THE COLUMNS
- USES THE FACT THAT THE COLUMN LINEAR MAPPINGS ARE INVERTIBLE
- USES THE FACT THAT ONE ADDITIONAL ROUND CAN BE "PEELED OFF" BY GUESSING RELATIVELY FEW KEY BITS

NONE OF THE ABOVE IS APPLICABLE TO OUR SASAS SCHEME.

10

## BIHAM'S ATTACK ON PATARIN'S SCHEME:

- ATTACKS ASASA, WHICH IS SLIGHTLY SIMPLER THAN OUR SASAS.
- CRUCIALLY DEPENDS ON THE FACT THAT RANDOM SYSTEMS OF MULTIVARIATE QUADRATIC EQUATIONS ARY TYPICALLY NON-INVERTIBLE
- REQUIRES ABOUT SQUARE ROOT OF THE NUMBER OF POSSIBLE PLAINTEXTS IN ORDER TO DETECT COLLISIONS IN THE VARIOUS S ELEMENTS.

BIHAM'S ATTACK IS IMPOSSIBLE TO APPLY TO SCHEMES WITH INVERTIBLE OPERATIONS, AND IS TOO COSTLY WHEN THE PLAINTEXTS CONTAIN AT LEAST 128 BITS.

11

## OTHER ATTACKS WHICH DO NOT APPLY TO SASAS:

- GUESS ONE ROUND AND VERIFY.
- MEET IN THE MIDDLE ATTACKS.
- DIFFERENTIAL ATTACKS.
- IMPOSSIBLE DIFFERENTIAL ATTACKS.
- TIME/MEMORY TRADEOFFS.
- ATTACKS BASED ON INCOMPLETE AVALANCHE.

.
.
.

12

# THE MAIN IDEA:

## USE A MULTISET ATTACK.

- IN DIFFERENTIAL ATTACKS, WE FOLLOW THE EVOLUTION OF DIFFERENCES BETWEEN TWO ENCRYPTIONS
- IN MULTISET ATTACKS, WE FOLLOW THE NUMBER OF TIMES VALUES OCCUR DURING THE ENCRYPTION OF A MULTISET OF INITIAL PLAINTEXTS.
- THE PROPERTIES WE USE:

(CONSTANT) **C**: A SINGLE VALUED REPEATED MULTIPLE TIMES
(PERMUTATION) **P**: EACH VALUE OCCURS EXACTLY ONCE
(EVEN) **E**: EACH VALUE OCCURS AN EVEN NUMBER OF TIMES
(BALANCED) **B**: XOR OF ALL VALUES (WITH MULTIPLICITIES) IS ZERO
(DUAL) **D**: EITHER P OR E

13

# IT IS EASY TO SHOW THAT:

- AN INVERTIBLE OPERATION CHANGES THE VALUES IN A MULTISET, BUT PRESERVES ITS MULTISET OF MULTIPLICITIES.
- A NON INVERTIBLE OPERATION CAN ONLY MERGE ENTRIES IN THE MULTISET OF MULTIPLICITIES.
- PROPERTY E OR P (WITH MORE THAN ONE BIT) IMPLY PROPERTY B.
- PROPERTIES E AND C ARE PRESERVED BY ARBITRARY MAPPINGS.
- PROPERTY P IS PRESERVED BY INVERTIBLE MAPPINGS
- PROPERTY B IS PRESERVED BY LINEAR MAPPINGS AND BY AFFINE MAPPINGS (WITH MORE THAN ONE BIT)

14

# WE CAN GENERALIZE THE MULTISET PROPERTIES TO A CONCATENATION OF BLOCK

EXAMPLES: $C^{i-1} P C^{k-i}$, $D^k$

NOTE: THIS IS A DECOMPOSITION PROPERTY, NOT A CROSS PRODUCT. THE DECOMPOSITION OPERATION IS IRREVERSIBLE SINCE WE LOSE THE ASSOCIATION.

IT IS EASY TO SHOW:

- PROPERTY $C^{i-1} P C^{k-i}$ IS PRESERVED BY A LAYER OF INVERTIBLE SBOXES.
- PROPERTY $D^k$ IS PRESERVED BY A LAYER OF INVERTIBLE SBOXES
- PROPERTY $D^k$ IS TRANSFORMED INTO PROPERTY $B^k$ BY AN ARBITRARY AFFINE MAPPING (WITH MORE THAN ONE BIT).
- PROPERTY $C^{i-1} P C^{k-i}$ IS TRANSFORMED INTO PROPERTY $D^k$ BY AN ARBITRARY AFFINE TRANSFORM (WITH MORE THAN ONE BIT)

15

# PROOF OF THE LAST TWO STATEMENTS:

PROOF OF: $D^k \xrightarrow[\text{AFFINE MAPPING A}]{} B^k$ (MORE THAN ONE BIT)

$P \xrightarrow[I]{} B$ (MORE THAN ONE BIT)

$E \xrightarrow[I]{} B$ (ALWAYS)

$D=(P \vee E) \xrightarrow[I]{} B$ (MORE THAN ONE BIT)

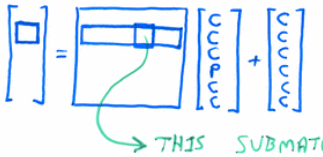
$D^k \xrightarrow[I]{} B^k$ (MORE THAN ONE BIT)

$B^k \xrightarrow[A]{} B^k$ (MORE THAN ONE BIT)

Q.E.D

16

PROOF OF: $C^{i-1} P C^{k-i} \xrightarrow[A]{\text{AFFINE}} D^k$ (>1 BIT)



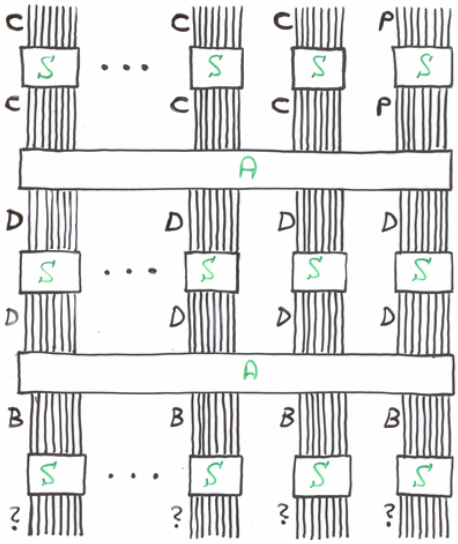
→ THIS SUBMATRIX MAY BE EITHER INVERTIBLE OR NON INVERTIBLE.

- IF INVERTIBLE, THE RESULTANT ENTRY IS F
- IF NON INVERTIBLE, THE SIZE OF THE KERNEL IS $2^i$ FOR SOME $i \geq 1$, WHICH IS EVEN, AND THUS EACH VALUE IS OBTAINED AN EVEN NUMBER OF TIMES, AND HAS PROPERTY E.
- SINCE EACH OUTPUT BLOCK IS EITHER P OR E, THE WHOLE OUTPUT IS $D^k$.

417

# THE STRUCTURE OF SASAS:

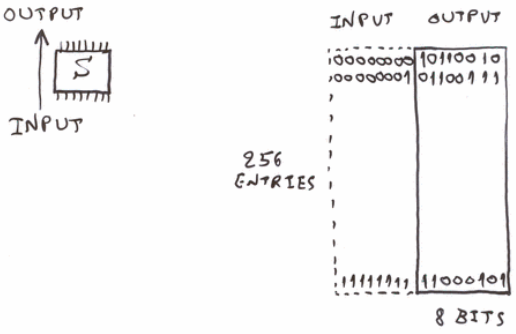
PUTTING IT ALL TOGETHER: THE ACTUAL MULTISET ATTACK WITH 256 CHOSEN PLAINTEXTS




18

# FINDING THE SBOXES AT THE BOTTOM:

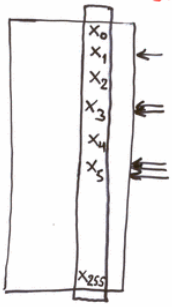
- CONSIDER EACH SBOX IN THE REVERSE DIRECTION AS A LOOKUP TABLE:




- WE ENCRYPTED 256 PLAINTEXTS
- WE KNOW THE 256 CIPHERTEXTS, WHICH POINT TO 256 ENTRIES (WITH REPETITIONS) INTO THIS UNKNOWN TABLE OF THE REVERSED SBOX.
- WE KNOW THAT THE XOR OF THE 256 ENTRIES IS ZERO, SO WE GET ONE RANDOM LOOKING HOMOGENEOUS LINEAR MAPPING!

19

TO GET ONE EQUATION USE CCC···CCP (256 CHOSEN PLAINTEXTS)




$$0 \cdot x_0 \oplus 1 \cdot x_1 \oplus 0 \cdot x_2 \oplus 0 \cdot x_3 \oplus 0 \cdot x_4 \oplus 1 \cdot x_5 \oplus \cdots = 0$$

TO GET 256 LINEAR EQUATIONS USE CCC···CPP ($2^{16}$ CHOSEN PLAINTEXTS)

EXPERIMENTAL RESULT: THE RANK OF THESE 256 LINEAR EQUATIONS IN 256 BINARY UNKNOWNS WAS ALWAYS 247.

EXPLANATION: THE SYSTEM IS INVARIANT UNDER:
- LINEAR MIXING OF THE COLUMNS
- COMPLEMENTATION.

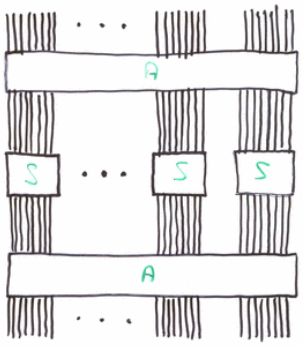
20

## THE ATTACK SO FAR:

- USE $2^{16}$ CHOSEN PLAINTEXTS TO FIND POSSIBLE VALUES FOR ALL THE SBOXES AT THE BOTTOM LAYER
- USE $2^{16}$ CHOSEN CIPHERTEXTS TO FIN POSSIBLE VALUES FOR ALL THE SBOXES AT THE TOP LAYER
- SOLVING THE SYSTEMS OF EQUATIONS TAKE SEVERAL SECONDS ON A SINGLE PC
- WE CAN "PEEL OFF" THE KNOWN LAYERS AND OBTAIN A SIMPLIFIED ASA SCHE

21

## THE ATTACK ON ASA:

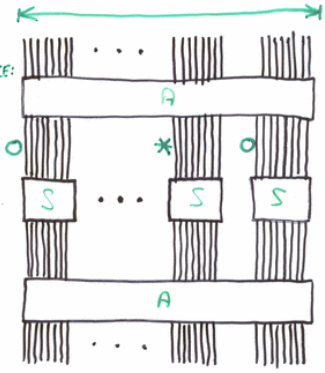



- INSTEAD OF FINDING THE INDIVIDUAL COMPONENTS, WE'LL FIND A COMPACT REPRESENTAT OF THIS TRANSFORMATION

22

## THE ATTACK ON ASA:

FINAL GOAL: FIND THE LINEAR SUBSPACE:




REPRESENT THE 128-DIM INPUT SPACE AS A DIRECT SUM OF 16 SUCH LINEAR SUBSPACES, EACH OF DIM 8.

THE ACTUAL OUTPUT IS THE XOR OF THE 16 VECTORS CONTRIBUTED FROM THE 16 SUBSPACES

FOR EACH VECTOR IN EACH SUBSPACE FIND ITS OUTPUT VECTOR BY A QUERRY

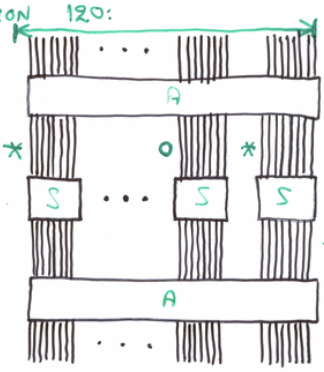
- INSTEAD OF FINDING THE INDIVIDUAL COMPONENTS, WE'LL FIND A COMPACT REPRESENTATION OF THIS TRANSFORMATION

PROBLEM: HOW CAN WE QUICKLY DETERMINE THE PARTITIONING OF THE 128 DIM SPACE INTO THE DIRECT SUM OF 16 SMALL 8-DIM SPACES.

23

## THE ATTACK ON ASA:

A LESS AMBITIOUS INTERMEDIATE GOAL: FIND SPACES OF DIMENTION 120:




PICK ARBITRARY $M_1$, $M_2$

THEN $M_1 \oplus M_2$ HAS DESIRED PROPERTY WITH PROB. $2^{-8}$.

TO VERIFY THAT $M_1$, $M_2$ ARE GOOD, TRY 256 RANDOM $M_3$

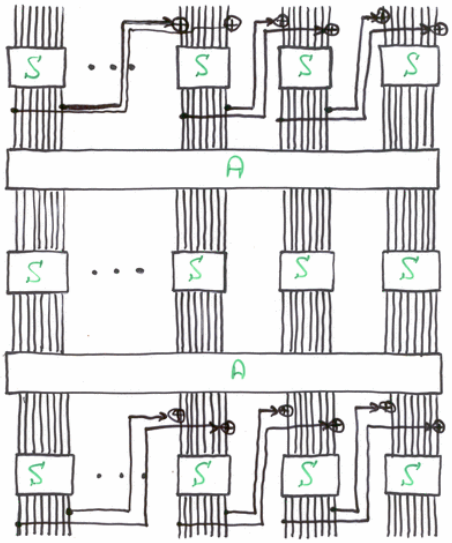
ENCRYPT $M_1 \oplus M_3$ AND $M_2 \oplus M_3$

ACCEPT $M_1$, $M_2$ IF THE SPACE SPANNED BY $E(M_1 \oplus M_2) \oplus E(M_2 \oplus M_3)$ IS ONLY 120-DIM.

- INSTEAD OF FINDING THE INDIVIDUAL COMPONENTS, WE'LL FIND A COMPACT REPRESENTATION OF THIS TRANSFORMATION
- AFTER FINDING 16 DIFFERENT 120-DIM INPUT SPACES, FIND THE 8-DIM INTERSECTION OF ANY 15 OUT OF THEM.
- GIVEN AN INPUT VECTOR, FIND ITS 16 PROJECTIONS, USE A TABLE LOOKUP FOR EACH ONE OF THEM, AND XOR THE RESULTS. THIS IS THE DESIRED COMPACT REPRESENTATION.

# THE STRUCTURE OF SASAS:

EXTENSION: ADD CHAINING TO SBOXES:

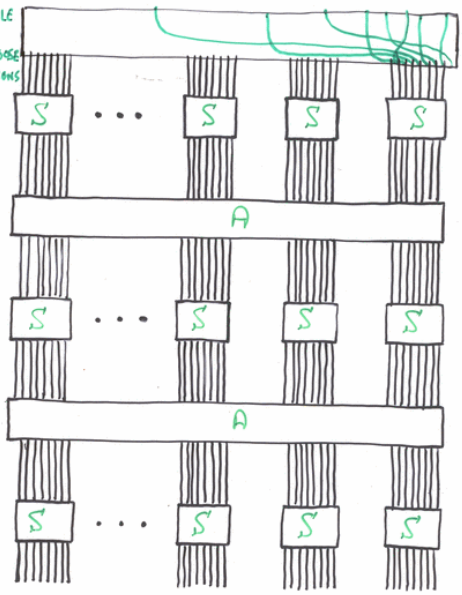





# THE STRUCTURE OF SASAS:

EXTENSION: ADD BIT PERMUTATION BEFORE/AFTE

$\binom{128}{8}$ POSSIBLE WAYS TO CHOOSE 8 LOCATIONS




REMARK: ADDING A FULL A LAYER BEFORE/AFTER REQUIRES GUESSING A $8 \times 128$ SLICE OF THE MATRIX, ADDING $2^{1000}$ TO THE COMPLEXITY