RusCrypto-2017

CREATING ASYMMETRIC SPN-CIPHER WITH WHITE-BOX CRYPTOGRAPHY AND CHAOTIC MAPS

PhD, Dmitry Schelkunov

Bauman Moscow State Technical University, Kaluga branch

White-box cryptography

- ✓ Allows to transform a symmetric block cipher to the asymmetric one by hiding a symmetric key in the obfuscated implementation (white-box implementation) of the encryption algorithm
- ✓ Aims to create fast asymmetric ciphers that allow both encryption and signing
- ✓ Would make a communication much lighter, faster and secure (there would be no need for Diffie-Hellman key exchange algorithm)
- ✓ One would communicate simultaneously with 2 and more others encrypting\decrypting a content "on-the-fly" without fear of the sender spoofing

Related work

- ✓Chow S., Eisen P., Johnson H., Van Oorschot P.C. (2003), **White-Box Cryptography and an AES Implementation**. In: Nyberg K., Heys H. (eds) Selected Areas in Cryptography. SAC 2002. Lecture Notes in Computer Science, vol 2595. Springer, Berlin, Heidelberg
- ✓Olivier Billet and Henri Gilbert. A Traceable Block Cipher. In Advances in Cryptology - ASIACRYPT 2003, volume 2894 of Lecture Notes in Computer Science, pages 331-346. Springer-Verlag, 2003
- ✓Olivier Billet, Henri Gilbert, and Charaf Ech-Chatbi. Cryptanalysis of a White-Box AES Implementation. In Proceedings of the 11th International Workshop on Selected Areas in Cryptography (SAC 2004), volume 3357 of Lecture Notes in Computer Science, pages 227–240. Springer-Verlag, 2004.
- ✓Brecht Wyseur, White-box cryptography, PhD thesis, March 2009
- ✓Dmitry Schelkunov, White-Box Cryptography and SPN ciphers. LRC method, Cryptology ePrint Archive: Report 2010/419
- ✓Brecht Wyseur, White-box cryptography: hiding keys in software, MISC magazine, April 2012
- ✓Joppe W. Bos and Charles Hubain and Wil Michiels and Philippe Teuwen, Differential Computation Analysis: Hiding your White-Box Designs is Not Enough, Cryptology ePrint Archive: Report 2015/753

Attacks on white-box implementations

Almost all attacks are based on separation of **known linear and non-linear parts** of the source symmetric cipher and added white-box transformations

- ✓Differential cryptanalysis (including fault injection)
- ✓Algebraic cryptanalysis
- ✓**Extraction of the non-linear part** (Olivier Billet, Henri Gilbert, and Charaf Ech-Chatbi. Cryptanalysis of a White-Box AES Implementation)

Method of concealing of a linear relationship

$$\begin{cases} x_1 = ((a \cdot b)(\text{mod } p_1) \cdot c)(\text{mod } p_2) \\ x_2 = (a \cdot (b \cdot c)(\text{mod } p_2))(\text{mod } p_1) \end{cases} \qquad (1)$$

$p_1, p_2 - \text{irreducible polynomials with degree } n$

$a, b, c, d, x_1, x_2 - \text{polinomials with degrees less than } n$

$$x_1 \neq x_2$$

Method of concealing of a linear relationship

$$\begin{cases} y_1(x) = (s(x)\cdot a(\text{mod } p_1))\cdot b(\text{mod } p_2) \\ y_2(x) = (s(x)\cdot c(\text{mod } p_1))\cdot d(\text{mod } p_3) \end{cases} \qquad (2)$$

p_1, p_2, p_3 – pairwice unequal irreducible polynomials over $GF(\alpha)$ with degree n

x, a, b, c, d – arbitrary polynomials over $GF(\alpha)$ with degrees less than n

$p_1, p_2, p_3, x, a, b, c, d$ are unknown

$y_1(x), y_2(x)$ are set as lookup tables

Method of concealing of a linear relationship

$$\begin{cases} y_1(x) = (s(x)\cdot a(\mathrm{mod}\ p_1))\cdot b(\mathrm{mod}\ p_2) \\ y_2(x) = (s(x)\cdot c(\mathrm{mod}\ p_1))\cdot d(\mathrm{mod}\ p_3) \end{cases} \qquad (2)$$

PROBLEM : find a linear relationship between

$s(x)\cdot a(\mathrm{mod}\ p_1)$ and $s(x)\cdot c(\mathrm{mod}\ p_1)$

Method of concealing of a linear relationship

$$\begin{cases} y_1(x) = (s(x)\cdot a - p_1 \cdot q_1)\cdot b (\mathrm{mod}\ p_2) \\ y_2(x) = (s(x)\cdot c - p_1 \cdot q_1')\cdot d (\mathrm{mod}\ p_3) \end{cases} \qquad (3)$$

$$\begin{cases} y_1(x) = s(x)\cdot a \cdot b - p_1 \cdot q_1 \cdot b - p_2 \cdot q_2 \\ y_2(x) = s(x)\cdot c \cdot d - p_1 \cdot q_1' \cdot d - p_3 \cdot q_3 \end{cases} \qquad (4)$$

$$q_1 = \left\lfloor \frac{s(x)\cdot a}{p_1} \right\rfloor; q_1' = \left\lfloor \frac{s(x)\cdot c}{p_1} \right\rfloor; q_2 = \left\lfloor \frac{s(x)\cdot a \cdot b - p_1 \cdot q_1 \cdot b}{p_2} \right\rfloor; q_3 = \left\lfloor \frac{s(x)\cdot c \cdot d - p_1 \cdot q_1' \cdot d}{p_3} \right\rfloor$$

PROBLEM: $y_1(x)$, $y_2(x)$ are known (lookup tables). Find a and c

RLWE?

Method of concealing of a linear relationship

Make (2) harder

$$\begin{cases} y_1(x) = (\ldots(s(x)\cdot a(\mathrm{mod}\ p_1))\cdot b^{(0)}(\mathrm{mod}\ p_2^{(0)})\ldots)\cdot b^{(k)}(\mathrm{mod}\ p_u^{(k)}) \\ y_2(x) = (\ldots(s(x)\cdot c(\mathrm{mod}\ p_1))\cdot d^{(0)}(\mathrm{mod}\ p_3^{(0)})\ldots)\cdot d^{(k)}(\mathrm{mod}\ p_v^{(k)}) \end{cases} \qquad (5)$$

$$p_i^{(\alpha)} \neq p_j^{(\alpha)}$$

$$\text{Hardness}: \min(2^{2n(k+1)}, (2^n!)^2)$$

Chaos theory in cryptography

- ✓Goce Jakimoski and Ljupˇco Kocarev, Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: FUNDAMENTAL THEORY AND APPLICATIONS, VOL. 48, NO. 2, FEBRUARY 2001
- ✓Asim, M., Jeoti, V.: Efficient and simple method for designing chaotic S-boxes. ETRI Journal 30(1), 170–172 (2008)
- ✓Mona Dara and Kooroush Manochehri, A Novel Method for Designing S-Boxes Based on Chaotic Logistic Maps Using Cipher Key. World Applied Sciences Journal 28 (12): 2003-2009, 2013
- ✓Christopher A. Wood, Chaos-Based Symmetric Key Cryptosystems
- ✓Dragan Lambić and Miodrag Živković, COMPARISON OF RANDOM S-BOX GENERATION METHODS. PUBLICATIONS DE L’INSTITUT MATHÉMATIQUE Nouvelle série, tome 93 (107) (2013)

Designing S-boxes with chaotic maps

- ✓ Good cryptographic properties
- ✓ Simple algorithms
- ✓ Random S-boxes with good cryptographic properties allow to increase a security of a white-box implementation

MDS codes and MDS matrix

MDS matrix (Maximal Distance Separable matrix) is a generating matrix of an MDS code

- Maximal diffusion by design
- Is used in SPN-ciphers in diffusion layers
- Interesting types of matrices:
  - Vandermonde matrix
  - Involutory matrix (the same MDS matrix for encryption and decryption)
  - **Cauchy matrix**
  - Circulant matrix (like in Rijndael)

Cauchy matrix

$$a_{ij} = \left(x_i + y_j\right)^{-1}; x_i + y_j \neq 0; 0 \leq i < m; 0 \leq j < n; x_i, y_j, a_{ij} \in GF\left(2^k\right)$$

- ✓MDS matrix by design
- ✓Simple algorithm of generation regardless of dimension
- ✓The property of circularity is not principal for the white-box implementation
- ✓The property of involutivity is harmful for the white-box implementation
- ✓**So, choose a Cauchy matrix**

A round of SPN-cipher

Add round key

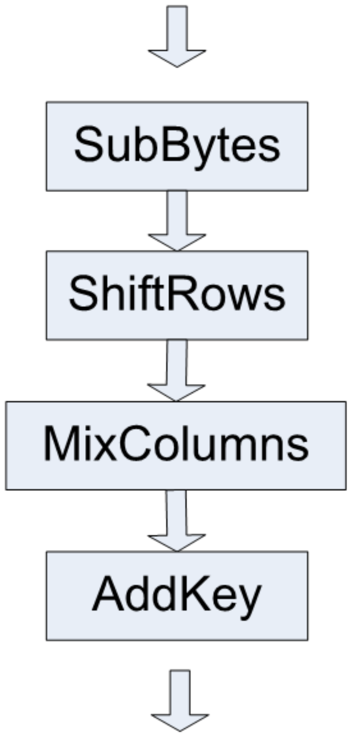
↓

Nonlinear part (S-boxes)

↓

Diffusion layer (MDS matrix + shifts)

A round of SPN cipher and T-boxes (Rijndael)



$$\begin{bmatrix} e_{0j} \\ e_{1j} \\ e_{2j} \\ e_{3j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \bullet \begin{bmatrix} S[a_{0j}] \\ S[a_{1j-1}] \\ S[a_{2j-2}] \\ S[a_{3j-3}] \end{bmatrix} \oplus \begin{bmatrix} k_{0j} \\ k_{1j} \\ k_{2j} \\ k_{3j} \end{bmatrix}$$

$$T_0[a] = \begin{bmatrix} S[a] \bullet 02 \\ S[a] \\ S[a] \\ S[a] \bullet 03 \end{bmatrix}; T_1[a] = \begin{bmatrix} S[a] \bullet 03 \\ S[a] \bullet 02 \\ S[a] \\ S[a] \end{bmatrix};$$

$$T_2[a] = \begin{bmatrix} S[a] \\ S[a] \bullet 03 \\ S[a] \bullet 02 \\ S[a] \end{bmatrix}; T_3[a] = \begin{bmatrix} S[a] \\ S[a] \\ S[a] \bullet 03 \\ S[a] \bullet 02 \end{bmatrix}$$

$$\begin{bmatrix} e_{0j} \\ e_{1j} \\ e_{2j} \\ e_{3j} \end{bmatrix} = T_0[a_{0j}] \oplus T_1[a_{1j-1}] \oplus T_2[a_{2j-2}] \oplus T_3[a_{3j-3}] \oplus \begin{bmatrix} k_{0j} \\ k_{1j} \\ k_{2j} \\ k_{3j} \end{bmatrix}$$

Chaotic asymmetric white-box SPN cipher

- ✓S-boxes (8x8 bits) are generated randomly (using chaotic maps) for the every of the input bytes of the every of the rounds
- ✓MDS matrix (16x16 bytes) is generated randomly (Cauchy matrix) for the every of the rounds
- ✓A white-box implementation is based on obfuscation of the T-boxes
- ✓A linear relationship between elements of the T-box is obfuscated with **method of concealing of a linear relationship**
- ✓A set of the obfuscated T-boxes is a public key

A round of the chaotic asymmetric white-box SPN cipher

$$Y_j = \begin{bmatrix} y_j^{(0)} \\ y_j^{(1)} \\ \dots \\ y_j^{(15)} \end{bmatrix} = \begin{bmatrix} mix_j^{(0)}(t_j^{(0,0)}(s_j^{(0)}(y_{j-1}^{(0)})) \\ mix_j^{(1)}(t_j^{(1,0)}(s_j^{(0)}(y_{j-1}^{(0)})) \\ \dots \\ mix_j^{(15)}(t_j^{(15,0)}(s_j^{(0)}(y_{j-1}^{(0)})) \end{bmatrix} \oplus \begin{bmatrix} mix_j^{(0)}(t_j^{(0,1)}(s_j^{(1)}(y_{j-1}^{(1)})) \\ mix_j^{(1)}(t_j^{(1,1)}(s_j^{(1)}(y_{j-1}^{(1)})) \\ \dots \\ mix_j^{(15)}(t_j^{(15,1)}(s_j^{(1)}(y_{j-1}^{(1)})) \end{bmatrix} \oplus \dots \oplus \begin{bmatrix} mix_j^{(0)}(t_j^{(0,15)}(s_j^{(15)}(y_{j-1}^{(15)})) \\ mix_j^{(1)}(t_j^{(1,15)}(s_j^{(15)}(y_{j-1}^{(15)})) \\ \dots \\ mix_j^{(15)}(t_j^{(315,15)}(s_j^{(15)}(y_{j-1}^{(15)})) \end{bmatrix} \quad (6)$$

$y_{j-1}^{(0)}$ – output byte of the previous round (or an input byte if $j = 0$)

$s_j^{(k)}$ – unique S-box

$t_j^{(l,k)}$ – multiplication on the appropriate element of the MDS matrix over $GF(2^8)$

$mix_j^{(15)}$ – obfuscation using method of concealing of a linear relationship

Hiding a linear relationship between elements of the T-box

$$T'_i[a] = \begin{bmatrix} ((...(t_i^{(0)}(a)\cdot b_i^{(0,0)})(\bmod p_i^{(0,0)})\cdot b_i^{(0,1)}(\bmod p_i^{(0,1)})...)\cdot b_i^{(0,k_0)}(\bmod p_i^{(0,k_0)})\oplus val_0 \\ ((...(t_i^{(1)}(a)\cdot b_i^{(1,0)})(\bmod p_i^{(1,0)})\cdot b_i^{(1,1)}(\bmod p_i^{(1,1)})...)\cdot b_i^{(1,k_1)}(\bmod p_i^{(1,k_1)})\oplus val_1 \\ ((...(t_i^{(2)}(a)\cdot b_i^{(2,0)})(\bmod p_i^{(2,0)})\cdot b_i^{(2,1)}(\bmod p_i^{(2,1)})...)\cdot b_i^{(2,k_2)}(\bmod p_i^{(2,k_2)})\oplus val_2 \\ ((...(t_i^{(3)}(a)\cdot b_i^{(3,0)})(\bmod p_i^{(3,0)})\cdot b_i^{(3,1)}(\bmod p_i^{(3,1)})...)\cdot b_i^{(3,k_3)}(\bmod p_i^{(3,k_3)})\oplus val_3 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ ((...(t_i^{(n)}(a)\cdot b_i^{(n,0)})(\bmod p_i^{(n,0)})\cdot b_i^{(n,1)}(\bmod p_i^{(n,1)})...)\cdot b_i^{(n,k_n)}(\bmod p_i^{(n,k_n)})\oplus val_n \end{bmatrix} \quad (7)$$

$t_i^{(n)}$ – element of the T-box before obfuscation

$b_i^{(j,u)}$ – randomly selected polinomial in $GF(2^h)$

$p_i^{(j,u)}$ – randomly selected irreducible polinomial with degree h over $GF(2)$

$$p_i^{(0,v)} \neq p_i^{(1,v)} \neq \dots \neq p_i^{(n,v)}$$

EVHEN. A chaotic asymmetric white-box cipher

- ✓Is named in honor of two greatest mathematicians: **Evariste Galois and Jules Henri Poincare**
- ✓Allows both encryption and signing of messages with a speed of a classical block cipher
- ✓A size of a public key: 640 Kbytes
- ✓Light requirements: 16 xors of 16-byte values per round. Only 3 operations: **memory read, xor and memory write**

Application

- ✓ IoT
- ✓ DRM
- ✓ **Everywhere**

Links

EVHEN source code: https://github.com/dmschelkunov/EVHEN

Author's blog: http://dschelkunov.blogspot.com

Author's e-mail: d.schelkunov@gmail.com