Uwierzytelnione szyfrowanie

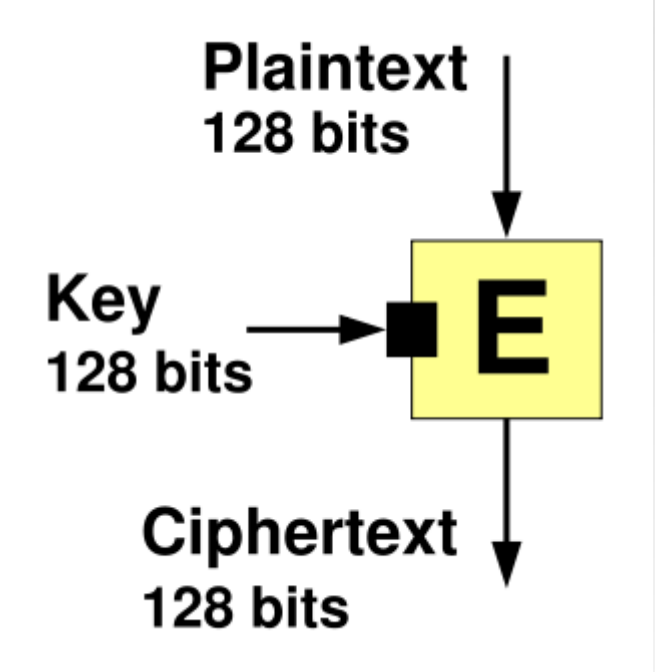
Paweł Szałachowski
pod kierunkiem: prof. Zbigniewa Kotulskiego

Plan prezentacji

- Szyfrowanie
  - podział, (pseudo)losowość, modele atakującego
- Tryby szyfrowania (poufność)
  - zalety, wady, ataki
- Uwierzytelnianie
  - schematy, właściwości
- Generic composition
- AEAD
  - iaPCBC, CCM, GCM, zastosowania
- Podsumowanie

Szyfrowanie - podział

- **Symetryczne**
  - **Blokowe**
  - Strumieniowe
- Asymetryczne



Model atakującego

- Atakujący: Maszyna Turinga ograniczona czasem wielomianowym
- Cele bezpieczeństwa:
  - IND – nierozróżnialność
  - NM – niemożność podszycia się
  - INT – integralność
- Ataki:
  - CPA – atak z wybranym tekstem otwartym
  - CCA1 – atak z wybranych tekstem zaszyfrowanym
  - CCA2 – adaptacyjny atak z wybranym tekstem zaszyfrowanym

Właściwości szyfru blokowego

- … lawinowość, brak: (auto)korelacji, kompresji, cech języka ...
- losowość (permutacji)

- Robert R. Coveyou: "Generowanie liczb losowych jest zbyt ważne, żeby zostawiać je przypadkowi"

Pseudolosowość

Idealny szyfr blokowy:

permutacja losowa (dla każdego klucza K, n -elem. perm.)

Dla każdego atakującego istnieje *negl(n)*:

P[D(p)=1] = ½ + negl(n)

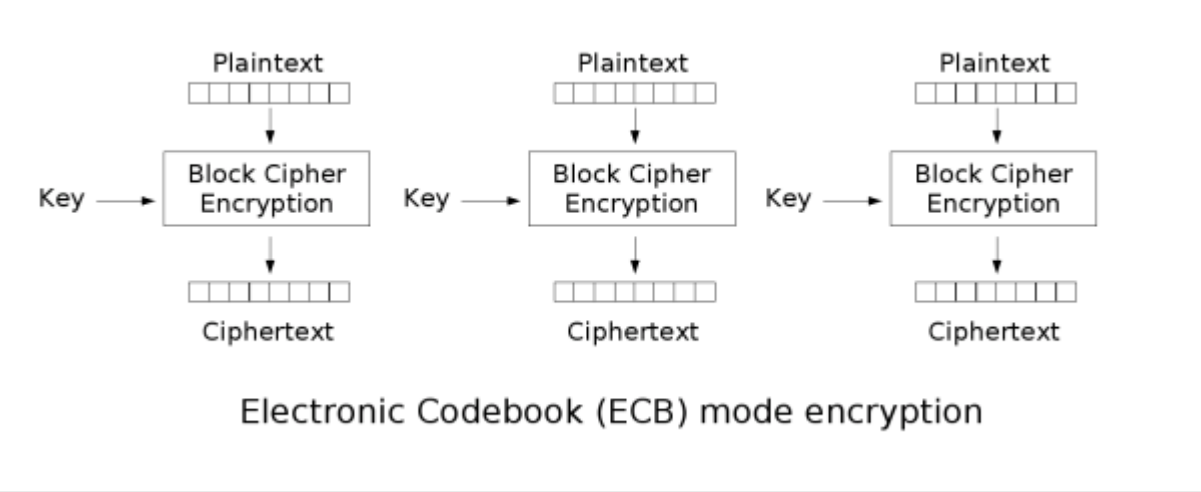
- **Atakujący:** *MT, O(n^c)*
- ***D(p)*** – return 1 jeśli atakujący trafnie określił czy permutacja jest losowa czy pseudolosowa
- ***P[D(p)=1]*** – prawdopodobieństwo odgadnięcia przez atakującego czy permutacja jest pseudolosowa
- ***negl(n)*** – funkcja parametru bezpieczeństwa (n), gdzie 1/negl(n) rośnie szybciej niż dowolna funkcja wielomianowa

Tryby szyfru blokowego

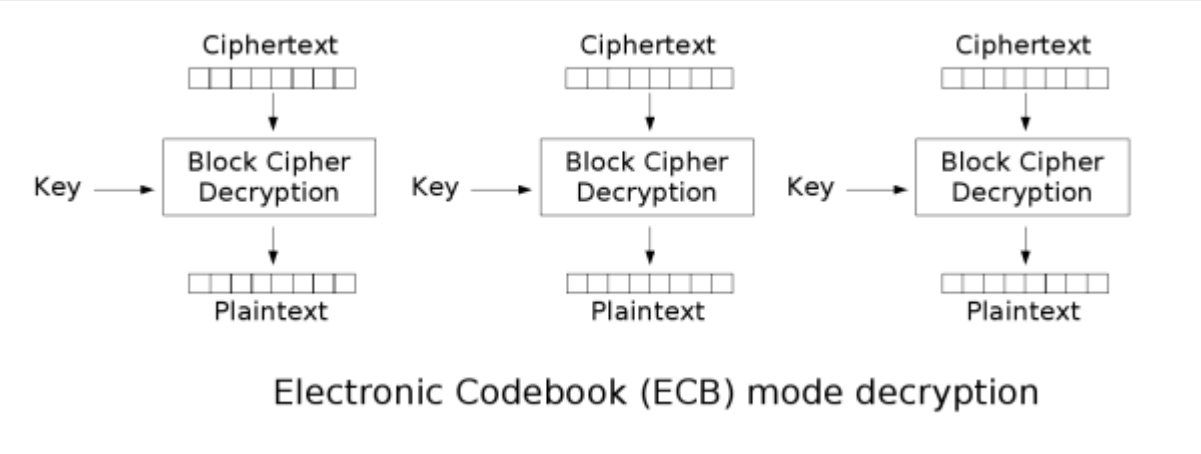
6 podstawowych trybów (**poufność - NIST**):

- ECB
- CBC
- OFB
- CFB
- CTR
- XTS-AES (storage devices)

Electronic codebook (ECB)



Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

ECB – scenariusz

- 64bity, uzgodniony klucz K, ”bezpieczna komunikacja”

  Alice przesyła **Bobowi** dokument techniczny fulltext342.pdf,

  Mallory obserwuje komunikację (znając dokument):

%PDF-1.2\n … **/Widths [675.93 937.5 875 787.04** **...**	**...** **136aa7b6c9ed916b 4e8dc6287ebf44f1** **519303ddc8383d14 9259894bf98aef14** **...**

ECB – scenariusz

- 64bity, uzgodniony klucz K, ”bezpieczna komunikacja”

  Alice przesyła **Bobowi** dokument techniczny fulltext342.pdf,

  Mallory obserwuje komunikację (znając dokument):

%PDF-1.2\n … **/Widths [675.93 937.5 875 787.04** **...**	**...** **136aa7b6c9ed916b 4e8dc6287ebf44f1** **519303ddc8383d14 9259894bf98aef14** **...**

Mallory wie, że Enc(K,”5 787.04”)= **9259894bf98aef14**

ECB - scenariusz

Alice wysyła (zaszyfrowane) **Bobowi**:

”Przelej 1 230.00 PLN na rachunek ...”

65011ea31d8ec018 1fb03e5c7a2cfb5a fbbdd4366e336e48 cc521fb484451b17

ECB - scenariusz

Alice wysyła (zaszyfrowane) **Bobowi**:

”Przelej 1 230.00 PLN na rachunek ...”

65011ea31d8ec018 1fb03e5c7a2cfb5a fbbdd4366e336e48 cc521fb484451b17

przyp. **Mallory** wie, że Enc(K,”5 787.04”)= **9259894bf98aef14**

Mallory zmienia 1fb03e5c7a2cfb5a na **9259894bf98aef14**

ECB - scenariusz

Alice wysyła (zaszyfrowane) **Bobowi**:

”Przelej 1 230.00 PLN na rachunek ...”

65011ea31d8ec018 1fb03e5c7a2cfb5a fbbdd4366e336e48 cc521fb484451b17

przyp. **Mallory** wie, że Enc(K,”5 787.04”)= **9259894bf98aef14**

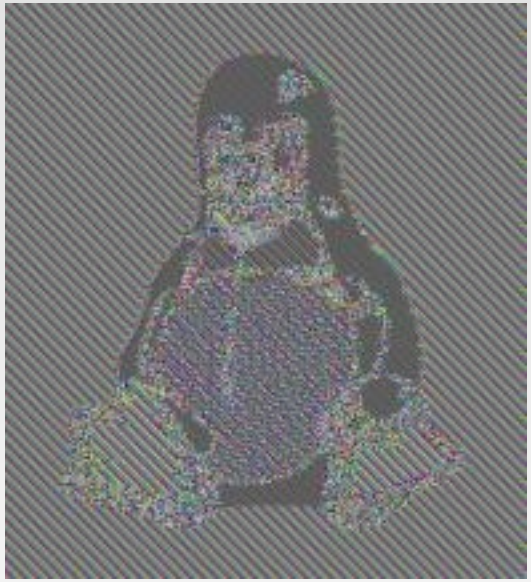
Mallory zmienia 1fb03e5c7a2cfb5a na **9259894bf98aef14**

Bob odszyfrowuje:

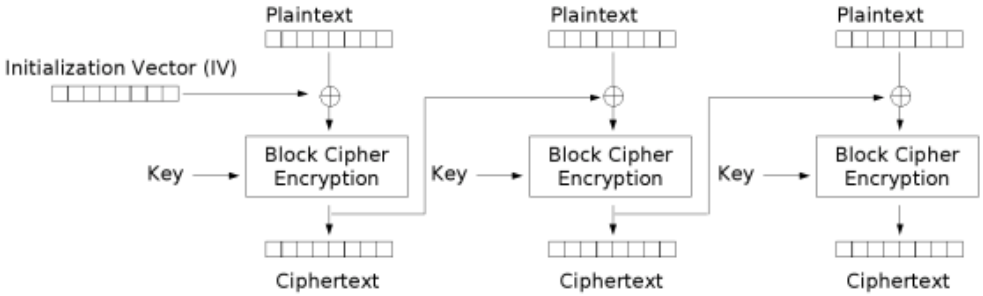
65011ea31d8ec018 **9259894bf98aef14** fbbdd4366e336e48 cc521fb484451b17

”Przelej 5 787.04 PLN na rachunek ...”

ECB – uwagi dot. bezpieczeństwa



Inne tryby poufności



Cipher Block Chaining (CBC) mode encryption

CBC:

Jeśli $C_i = C_j$ to:

$Enc(P_i \text{ xor } C_{i-1}) = Enc(P_j \text{ xor } C_{j-1})$

$P_i \text{ xor } C_{i-1} = P_j \text{ xor } C_{j-1}$

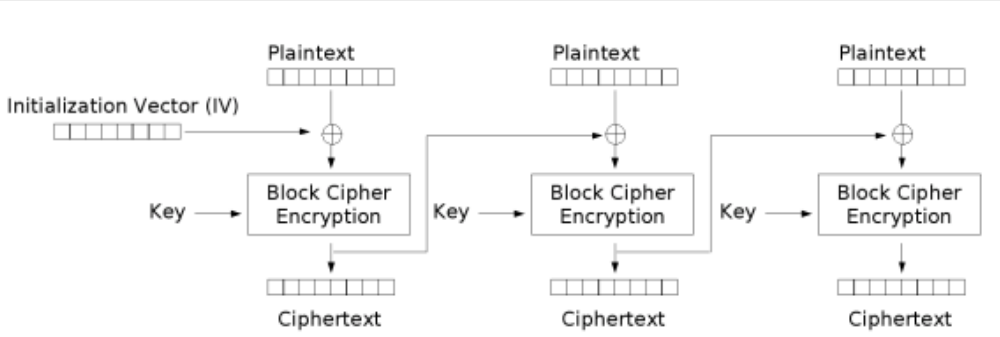
$P_i \text{ xor } P_j = C_{i-1} \text{ xor } C_{j-1}$

Jeśli $C_i \mathrel{!}= C_j$ to:

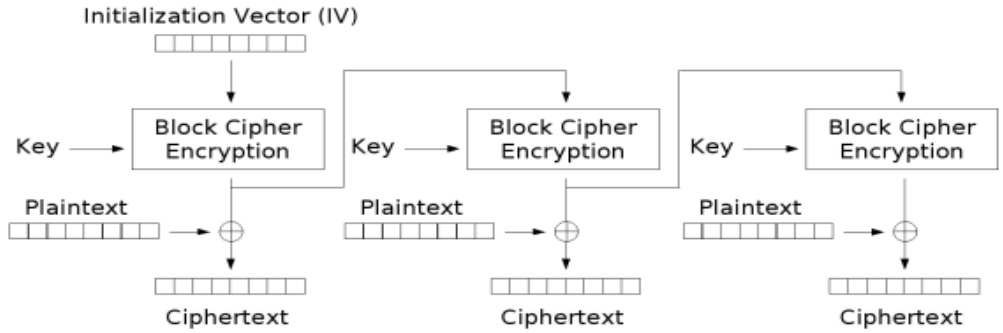
$P_i \text{ xor } P_j \mathrel{!}= C_{i-1} \text{ xor } C_{j-1}$

M-bloków n długości, ilość kolizji: ~ M(M-1)/2^(n+1)

Inne tryby poufności



Cipher Block Chaining (CBC) mode encryption



Output Feedback (OFB) mode encryption

CBC:

Jeśli $C_i = C_j$ to:

$Enc(P_i \text{ xor } C_{i-1}) = Enc(P_j \text{ xor } C_{j-1})$

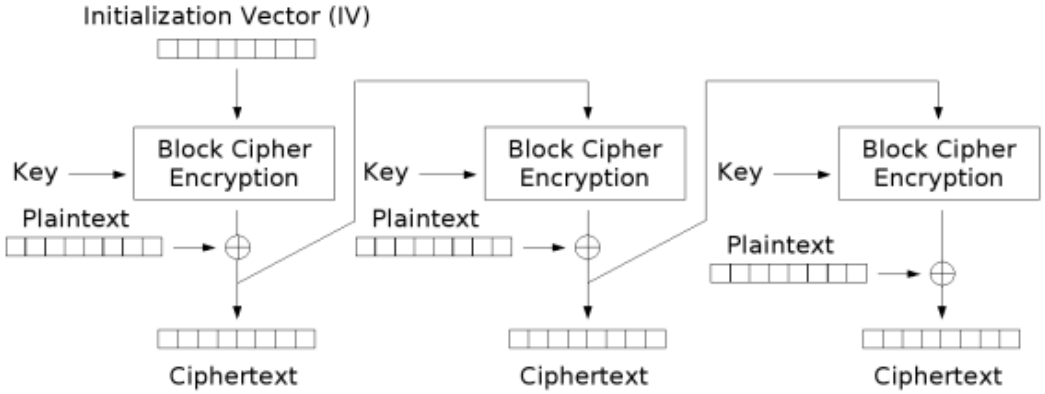
$P_i \text{ xor } C_{i-1} = P_j \text{ xor } C_{j-1}$

$P_i \text{ xor } P_j = C_{i-1} \text{ xor } C_{j-1}$

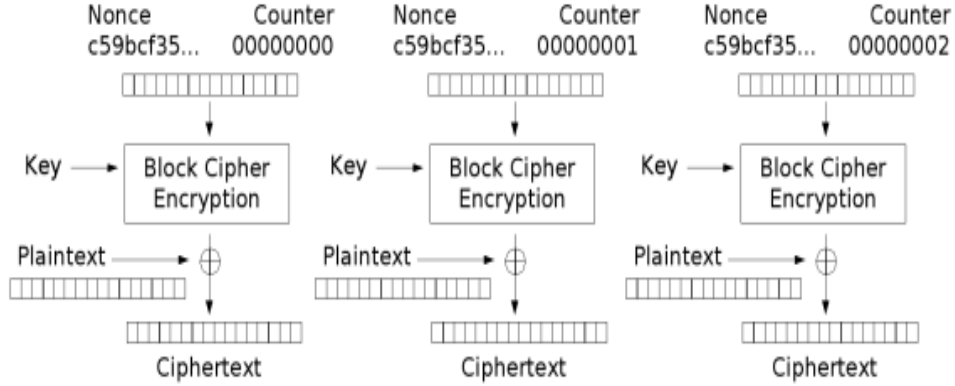
Jeśli $C_i != C_j$ to:

$P_i \text{ xor } P_j != C_{i-1} \text{ xor } C_{j-1}$

M-bloków n długości, ilość kolizji: ~ M(M-1)/2^(n+1)

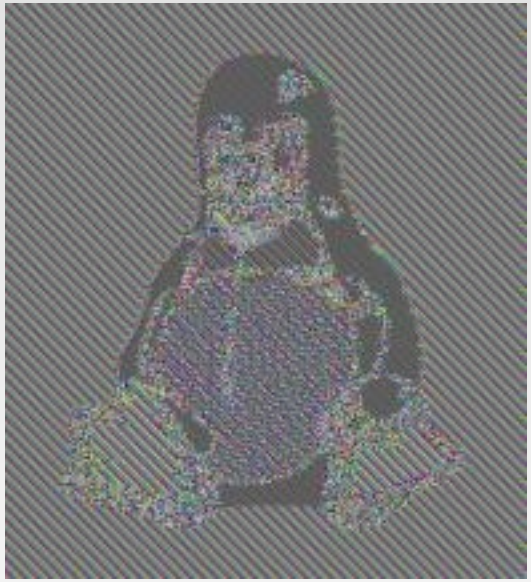


Cipher Feedback (CFB) mode encryption



Counter (CTR) mode encryption

Inne tryby poufności



Inne tryby poufności – podobne problemy

- ataki na IV, skrócenie szyfrogramu, wycieki informacji, kolizje wewnętrzne, …
- S.M. Bellovin ”Problem Areas for the IP Security Protocols”, 1996
- H. Krawczyk ”The Order of Encryption and Authenticationfor Protecting Communications (Or: how secure is SSL)”, 2001
- N. Borisov, I. Goldberg, D. Wagner ”Intercepting Mobile Communications: The Insecurity of 802.11”, 2001

- Poufność nie wystarcza.

Wiadomości trzeba uwierzytelniać!!!

Uwierzytelnianie

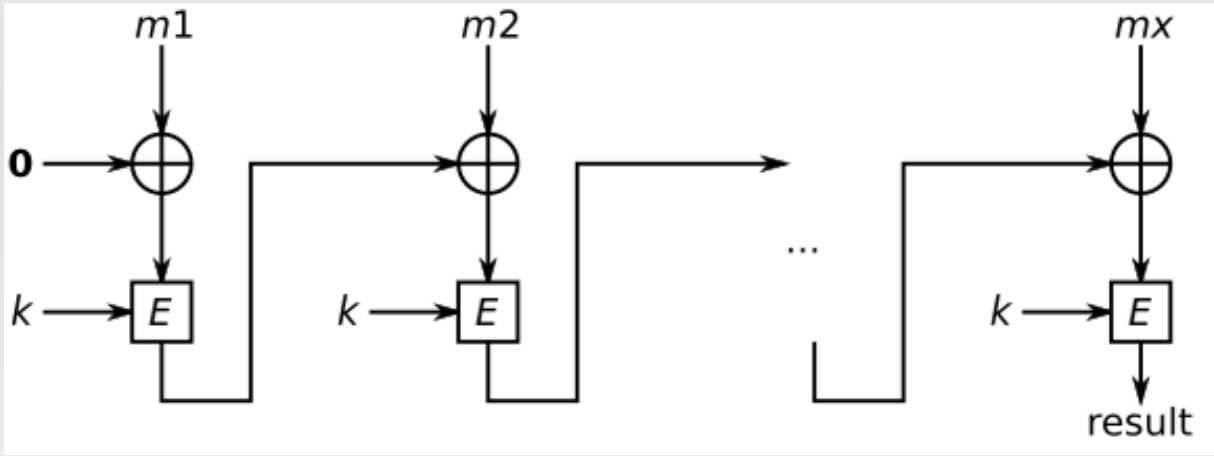
- *HMAC(K,M) = H[(K xor opad)* || *H[(K xor ipad)* || *M]]*

Uwierzytelnianie

- *HMAC(K,M) = H[(K xor opad)* || *H[(K xor ipad)* || *M]]*
- CBC-MAC

  CMAC, OMAC,

  UMAC,...



Bezpieczny jedynie dla wiadomości o ustalonej długości.

- Atakujący zna: *(m, t), (m', t')*. Może stworzyć *(m'',t'): m''=m* || *(m' xor t)*
- Użycie tego samego klucza do Enc() i Auth(): ZABRONIONE.

Construct	atk	Previous bound	Our bound
CBC	pf	$\ell^2 q^2/2^n$ [2, 13, 15]	$\ell q^2/2^n \cdot (12 + 64\ell^3/2^n)$
ECBC	any	$2.5\,\ell^2 q^2/2^n$ [7]	$q^2/2^n \cdot (d'(\ell) + 32\ell^4/2^n)$

Figure 1: Bounds on $\mathbf{Adv}^{\mathsf{pf}}_{\mathrm{CBC}}(q, n, \ell)$ and $\mathbf{Adv}^{\mathsf{any}}_{\mathrm{ECBC}}(q, n, \ell)$.

M. Bellare, K. Pietrzak, P. Rogaway ”Improved Security Analyses for CBC MACs”, 2005

Generic composition

Metoda	Protokół	Operacje	Transfer
AtE	SSL	a = Auth(m), C = Enc(m||a)	C
EtA	IPSec	C = Enc(m), a = Auth(C)	C||a
E&A	SSH	C = Enc(m), a = Auth(m)	C||a

- H. Krawczyk ”The Order of Encryption and Authentication for Protecting Communications”

- M. Bellare, C. Namprempre ”Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm”, 2007

E&A insecure: IND-CPA, IND-CCA, NM-CPA, INT-CTXT
AtE insecure: IND-CCA, NM-CPA, INT-CTXT

- D. Wagner, B. Schneier ”Analysis of the SSL 3.0 protocol”

AEAD (Authenticated Encryption with Associated Data)

- iaPCBC – V.Gligor, P.Donescu 1999
- P. Rogaway, 2002r
- IACBC, IAPM – C. Jutla, 2000r
- Połączenie funkcji trybów gwarantujących **Poufność** i **Uwierzytelnianie**
  - one-pass
  - two-pass

  - Dwa tryby (NIST): CCM, GCM/GMAC

iaPCBC

- iaPCBC – V.Gligor, P.Donescu, 1999

  R_0 dla każdego pakietu

  $C_0=Enc(KI, R_0)$ $\quad\quad$ $R_i=R_{i-1}+P_{i-1}+C_{i-1}$

  $P_0=Enc(KI,R_0 + 1)$ $\quad\quad$ $C_i=Enc(KD, M_i \text{ xor } R_i)$

  KV (np. SPI i SN IPsec)

  $M_{1..n}$ = Plaintext || KV $\quad\quad$ Przesyłamy $C_0 \ldots C_n$

  Odbiorca weryfikuje KV

- N.Ferguson, D. Whiting, J. Kelsey, D.Wagner ”Critical Weaknesses of iaPCBC”, 1999

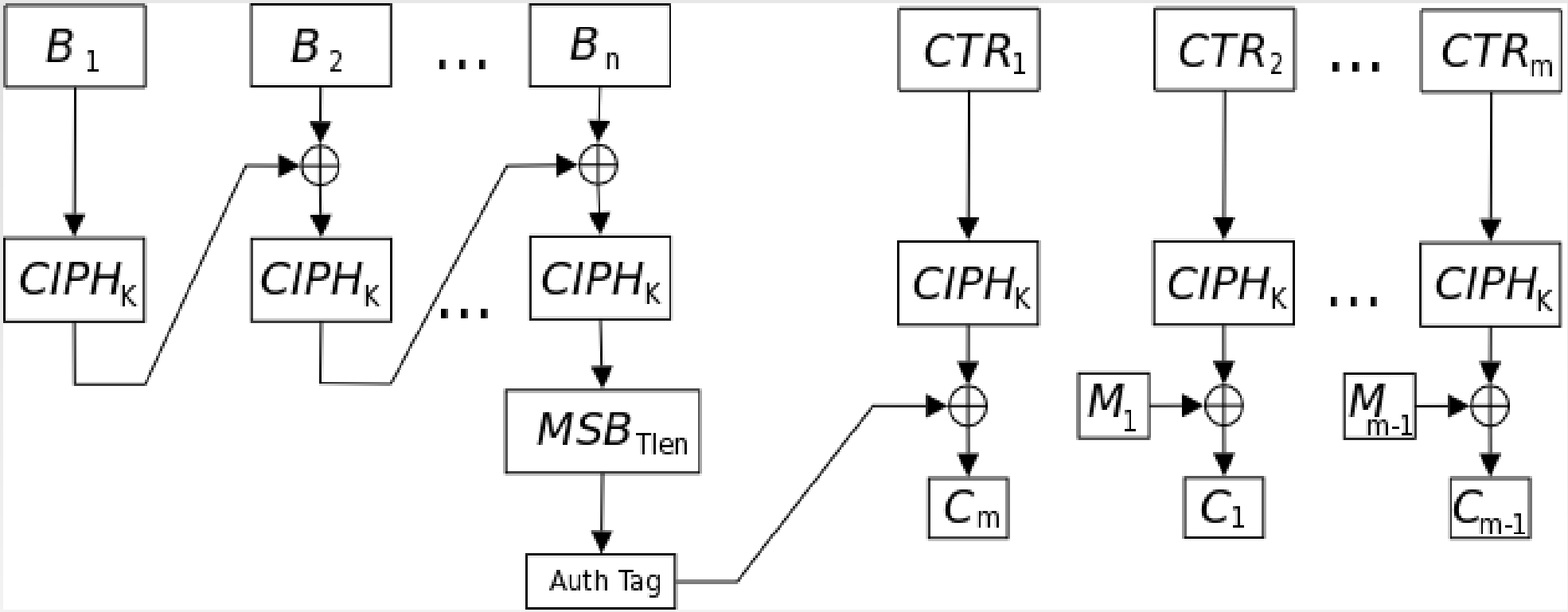
  ...

  M' = M || KV || Cokolwiek

  ...

Counter with CBC-MAC (CCM)

two-pass mode



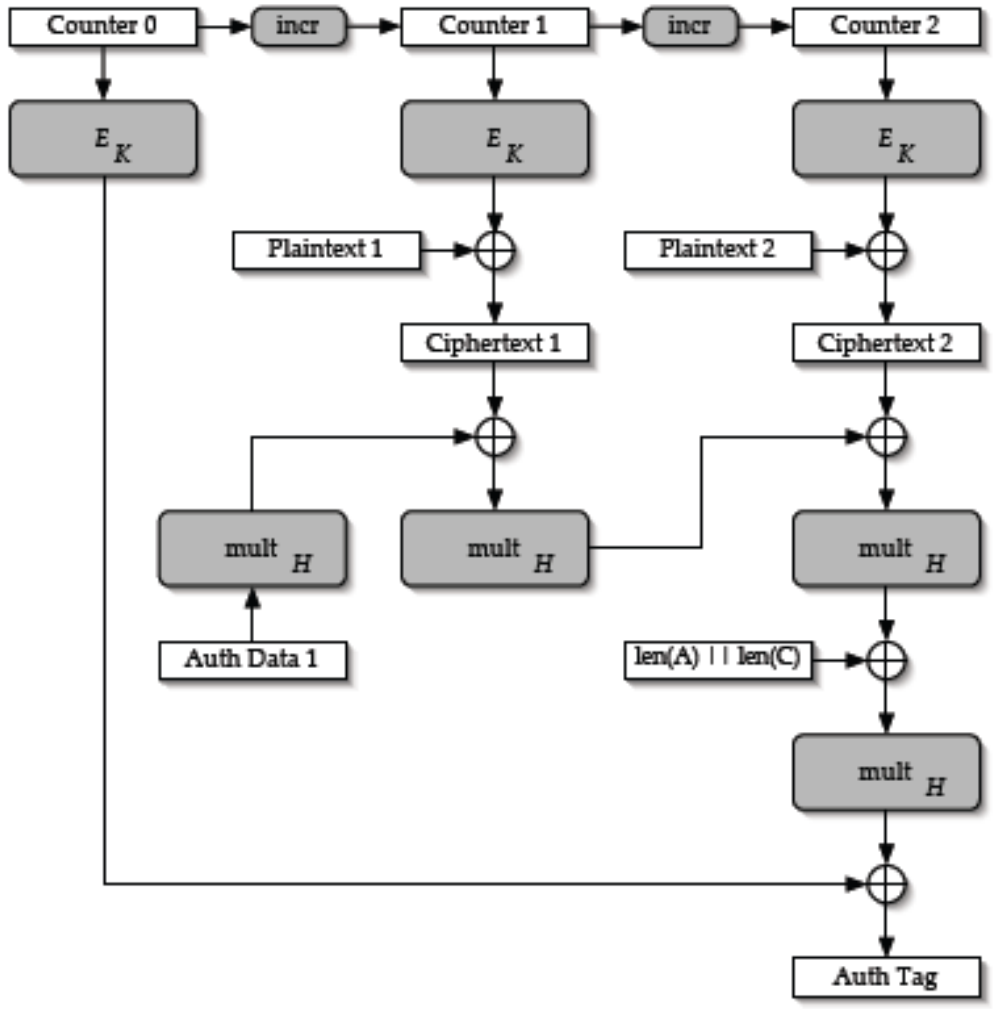
Jakob Jonsson, ”On the Security of CTR + CBC-MAC”
P. Rogaway, D. Wagner, ”A Critique of CCM”, 2003

Galois/Counter Mode (GCM/GMAC)

- może uwierzytelniać bez szyfrowania (GMAC)

- A. Joux ”Authentication Failures in NIST version of GCM”

- N. Ferguson ”Authentication weaknesses in GCM”, 2005



Zastosowanie trybów AuthEnc

- RFC 4106 The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
- RFC 4543 The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH
- RFC 5647 AES Galois Counter Mode for the Secure Shell Transport Layer Protocol
- RFC 5288 AES Galois Counter Mode (GCM) Cipher Suites for TLS
- RFC 4309: Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)
- **Wireless Sensor Networks**

WSN

- Tani i ”ograniczony” sprzęt
- Otwarte medium
- Autonomiczność
- ”self-healing”, ”self-configuration”
- …

- **Konieczność bezpiecznej komunikacji**

WSN a tryby zaawansowane

- **Wydajność** (zależna od implementacji)
- Poufność, Integralność i Uwierzytelnianie w jednej operacji kryptograficznej
- Wystarczy nam kod szyfru blokowego (a nawet jedynie funkcja szyfrowania)
- Podział danych względem operacji kryptograficznych:
  - nagłówek: uwierzytelniony
  - zawartość: uwierzytelniona i zaszyfrowana

WSN a tryby zaawansowane

Table 1
Performance of authenticated encryption modes.

Mode	Code size	Init	Size of AAD and payload (in bytes)											
			AAD	P	AAD	P	AAD	P	AAD	P	AAD	P	AAD	P
			8	16	8	32	8	64	16	16	16	32	16	64
CCM	4122 B	2597	658.79		560.15		489.63		592.50		532.39		479.98	
GCM	5706 B	21 085	984.50		842.22		747.37		736.28		700.45		671.80	
GCM-256B	6220 B	25 109	737.62		644.72		582.79		551.12		535.87		523.67	
GCM-4KB	10 271 B	57 686	500.62		455.12		424.79		373.37		377.87		381.47	
GCM-8KB	14 108 B	201 429	407.25		380.42		362.54		303.34		315.62		325.45	
EtM CMAC	3971 B	4211	505.70		438.87		401.44		466.46		423.93		396.13	

Table 2
Performance of authentication modes.

Mode	Code size	Init	Message size (in bytes)			
			16	32	48	64
CMAC	2240 B	5559	190.37	179.90	176.25	175.14
GMAC	5706 B	21 085	847.93	616.25	543.29	506.51
GMAC-256B	6220 B	25 109	601.06	431.09	378.79	352.21
GMAC-4KB	10 271 B	57 686	365.75	253.34	220.70	204.09
GMAC-8KB	14 108 B	201 429	270.68	183.31	158.45	145.73

P.Szalachowski, B.Ksiezopolski, Z.Kotulski, - *CMAC, CCM and GCM/GMAC: advanced modes of operation of symmetric block ciphers in the Wireless Sensor Networks* - Elsevier: Information Processing Letters, Vol.110, No.7, pp.247-251, (2010).;

WSN - uwierzytelnianie

Mode	Code size	Init	Message size (in bits)			
			128	256	384	512
CMAC	2240B	0.7ms	0.4ms	0.7ms	1.0ms	1.4ms
GMAC	5706B	2.6ms	1.7ms	2.5ms	3.2ms	4.0ms
GMAC-256B	6220B	3.1ms	1.2ms	1.7ms	2.3ms	2.8ms
GMAC-4KB	10271B	7.2ms	0.7ms	1.0ms	1.3ms	1.6ms
GMAC-8KB	14108B	25.1ms	0.5ms	0.7ms	0.9ms	1.2ms
HMAC-SHA1	5252B	0.0ms	4.7ms	4.7ms	4.8ms	4.8ms
HMAC-MD5	6348B	0.0ms	3.6ms	3.6ms	3.7ms	3.7ms
ECDSA sign	19308B	3493.4ms	2001.6ms	2001.6ms	2001.6ms	2001.6ms
ECDSA verify	19308B	3493ms	2436.5ms	2436.5ms	2436.5ms	2436.5ms

P.Szalachowski, B.Ksiezopolski, Z.Kotulski, ”On authentication method impact upon data sampling delay in Wireless Sensor Networks” - CN 2010, CCIS, Vol.79, pp.280-289, Springer-Verlag, Berlin Heidelberg 2010. ISBN 978-3-642-13860-7

Dziękuję za uwagę.
Pytania?