Authenticated and Misuse-Resistant Encryption of Key-Dependent Data

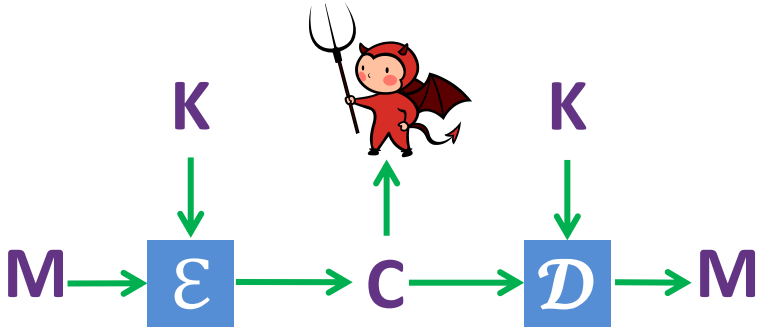
Mihir Bellare **Sriram Keelveedhi**

University of California, San Diego

Full version of this work appears in the Cryptology ePrint Archive

Classical Security: IND-CPA [GM84, BDJR97]

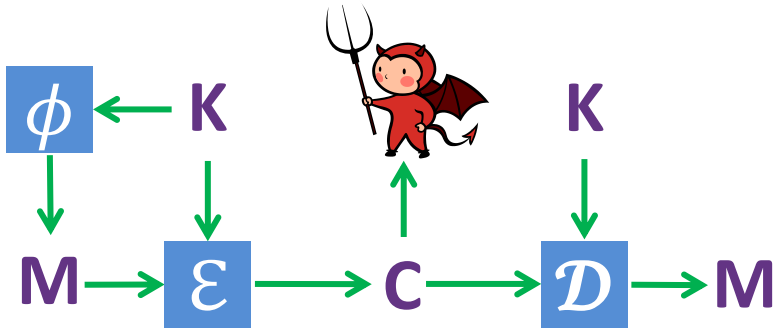
Caveat: Messages do not depend on the key



Key Dependent Messages

[CL01] Applications to anonymous credentials

[BRS02] Connections to formal methods



Key-dependent messages in practice

Disk encryption (BitLocker): Encryption key could reside on disk

Password, password hash could be stored on the system

IEEE 1619: KDM attack on LRW influenced its rejection

KDM-secure encryption is more misuse-resistant

Previous Work

[BRS02]



- Model and definitions for KDM-CPA secure encryption
- RO model solution $\mathcal{E}(K, R, M) = H(K||R) \oplus M$

Standard Model KDM secure encryption schemes

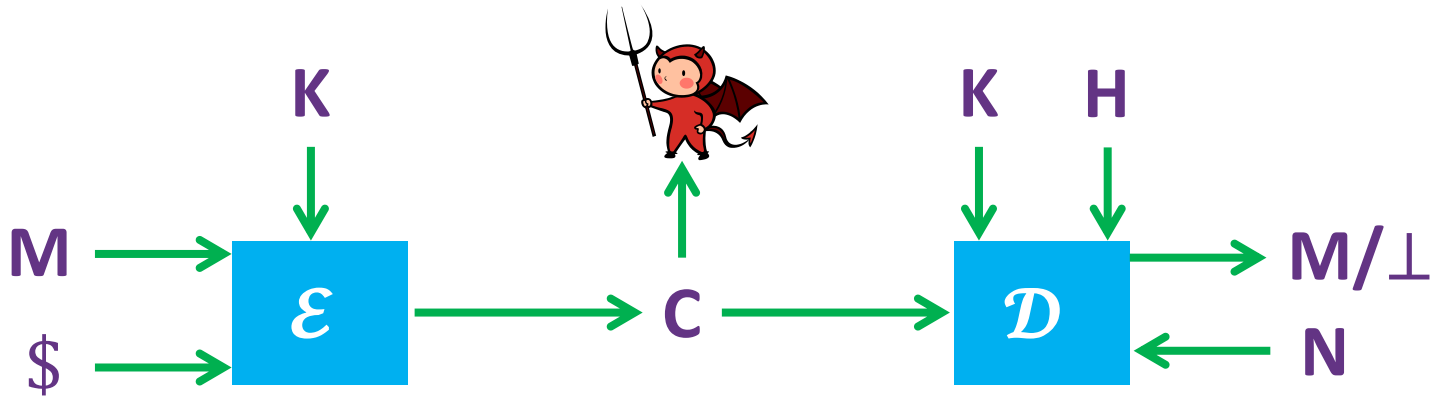
[BHHO08, BHHI10, BGK11, ACPS09, BG10, MTY11]

- Restricted classes of message deriving functions
- Inefficient

KDM for other primitives

- Limited KDM security for PRFs/PRPs **[HK07]**
- Basic form of AE **[BPS07]** ⟵ **Revisit**

[BPS07] considered classical AE

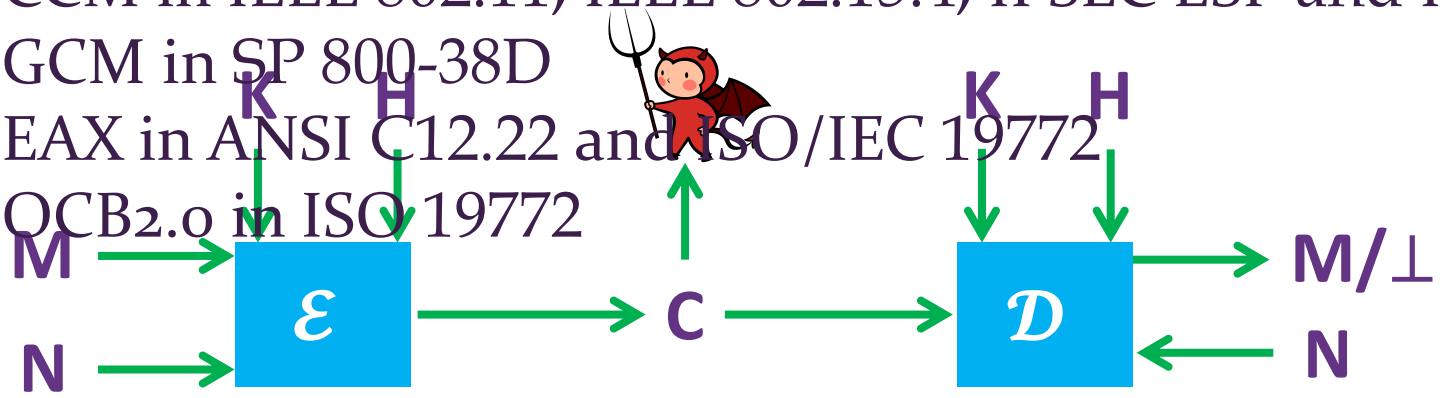


Privacy and Integrity of message **M**

Standards are of this form

Modern/in practice AE is more complex

- CCM in IEEE 802.11, IEEE 802.15.4, IPSEC ESP and IKEv2;
- GCM in SP 800-38D
- EAX in ANSI C12.22 and ISO/IEC 19772
- OCB2.0 in ISO 19772



Only Integrity of header **H**

Issues

- Message (M): key-dependent (kd) or key-independent (ki)
- Header (H): key-dependent (kd) or key-independent (ki)
- Security: Random nonce or universal nonce

Security notion	Nonce/IV (N)
Random nonce security	Should be randomly generated
Universal nonce security	Any non-repeating sequence will do

AE variants

- Message (M): key-dependent (kd) or key-independent (ki)
- Header (H): key-dependent (kd) or key-independent (ki)
- Security: Random nonce or universal nonce

Security	M: kd H: kd	M: kd H: kd	M: kd H: kd	M: kd H: ki
Random nonce	Yes	?	?	?
Universal nonce	Yes	?	?	?

We ask: When is security achievable?

[BPS07] M: kd; H: none

Our Contributions

- Simple unified definitions of security encompassing all variants of AE under KDM
- **Attacks:**
  - **NO** scheme secure with universal nonces
  - **NO** scheme secure with key dependent headers
- **RHtE**: Security under **M:kd; H:ki**

Standard AE Scheme KDM Secure AE Scheme

- **Features:**
  - Minimal computational overhead
  - Zero bandwidth overhead
  - Simple software changes
- **Security:** RO model solution

Recall: AE Security

$b \xleftarrow{\$} \{0,1\}$

$K \xleftarrow{\$} \{0,1\}^k$

es,

$\mathcal{AE} = (k, \mathcal{E}, \mathcal{D})$

Univer

Rando

I know b!

Challenger

K b

Decrypt N, C

Encrypt N, M

Use my nonce N

N', C'

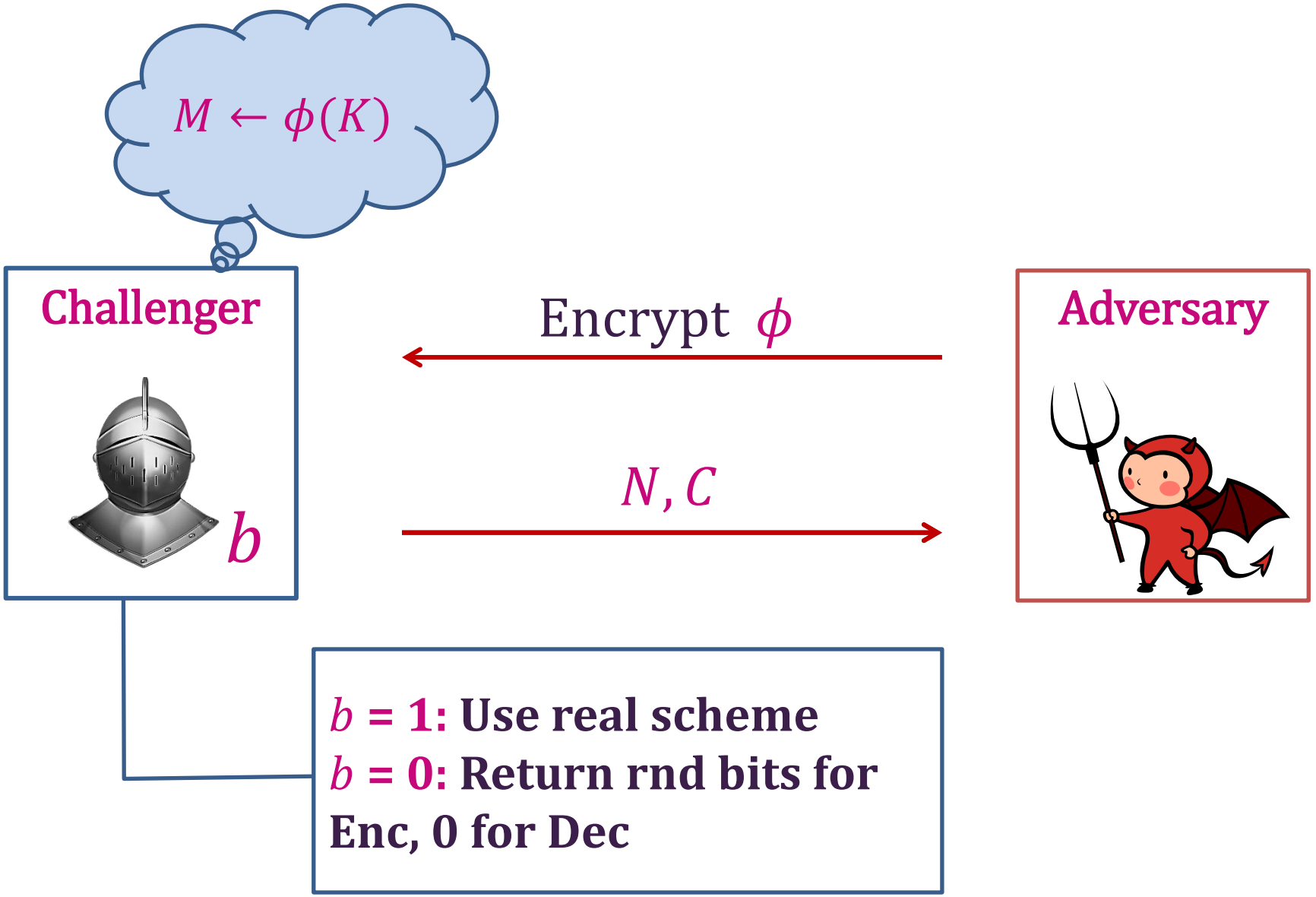
N', M'

Adversary

b = 1: Use real scheme

b = 0: Return rnd bits for Enc, 0 for Dec

KDM Security

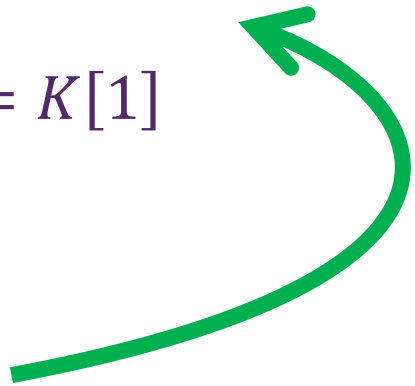


Universal nonce KDM-secure AE is impossible

Starting point: [BRS02] attack on stateful encryption

- Adversary gets to choose nonce
- Embed nonce N in ϕ
- ϕ knows N, K
  - Can simulate encryption of any message

Adversary A	$\phi_{S,N}(K)$
$N \xleftarrow{\$} \{0,1\}^r; S \xleftarrow{\$} \{0,1\}^s$ $(N, C) \leftarrow \mathbf{Enc}(N, \phi_{S,N})$ $K[1] \leftarrow S \cdot C$	Find M s. t $S \cdot \mathcal{E}(K, N, M) = K[1]$



Problem: How long will it take to find M?

Our Attack

- $F: \{0,1\}^s \times \{0,1\}^c \to \{0,1\}$ family of pairwise independent hash functions
- $m_1, m_2, \ldots$ list of all m-bit messages

Adversary A	$\boldsymbol{\phi_{s,\,i,\,N}(K)}$

$N \leftarrow 0;\ S \xleftarrow{\$} \{0,1\}^s$
For $i = 1, \ldots k$ do
$(N_i, C_i) \leftarrow \mathbf{Enc}(N, \epsilon, \phi_{s,\,i,\,N})$
$N \leftarrow N + 1$
$L[i] \leftarrow F(S, C_i)$
$//L = K$ w.h.p
	For $j = 1, \ldots l$ do
	$C \leftarrow \mathcal{E}(K, N, m_j)$
	If $K[j] = F(S, C)$ then
	Ret m_j
	Ret m_1

Claim: If $l = o(k)$, $\Pr[L \neq K] \leq \frac{1}{4}$

AE variants: Revisit

- No scheme secure with universal nonces
- No scheme secure with key-dependent headers

Security	M: kd H: kd	M: ki H: kd	M: kd H: ki
Random nonce	No	No	Yes
Universal nonce	No	No	No

RHtE

Message(M) , Header (H): key-dependent (kd) or key-independent (ki)

- No: Full KDM security is not possible

RHtE: RANDOMIZE, HASH then ENCRYPT

Standard AE Scheme KDM Secure AE Scheme

Hash function $F: \{0,1\}^* \rightarrow \{0,1\}^k$

$\overline{\mathcal{E}}(L,R,H,M)$	$\overline{\mathcal{D}}(L,R,H,C)$
$K \leftarrow F(L\|\|R)$ $C \leftarrow \mathcal{E}(K,H,M)$ Return C	$K \leftarrow F(L\|\|R)$ $M \leftarrow \mathcal{D}(K,H,C)$ Return M

- Minimal computational overhead
- Zero bandwidth overhead
- Simple software changes

Questions?