Reconsidering generic composition

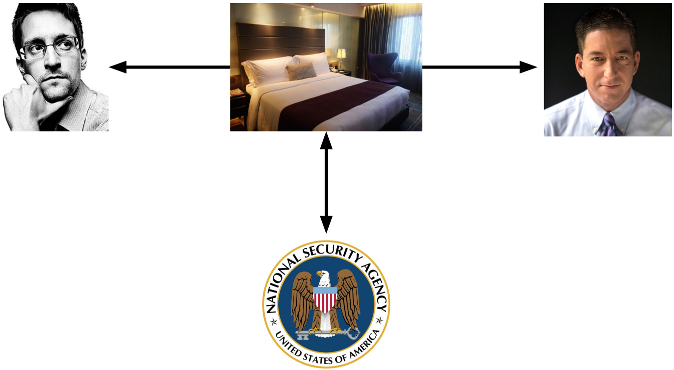
Vincent Loup

EPFL

May 29, 2017

Table of contents

We want to ensure messages are unaltered and confidential.



Authenticated encryption is the solution to this problem.

Authenticated Encryption (AE)

AE provides

- Confidentiality
- Integrity
- Authentication

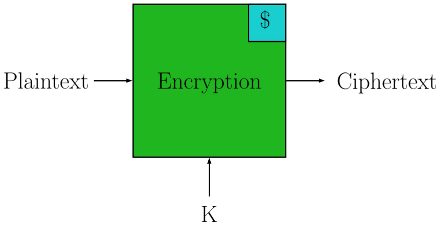
Generic composition: construction of Authenticated Encryption with an encryption scheme and a MAC.
Dedicated schemes: CCM, GCM or the ongoing CAESAR competition also provide authenticated encryption.

Generic composition

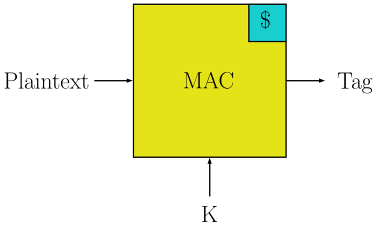
- Combine a MAC and an encryption scheme together as black boxes.
- Uses off the shelves schemes.
- First results in 2000, problem revisited in 2014.

Probabilistic schemes

First results of 2000 assumes we have probabilistic schemes.



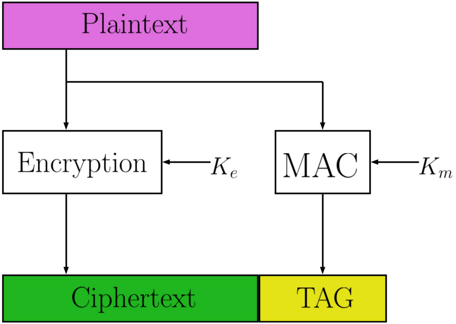
$E(K_e, M) = C$



$T(K_m, M) = Tag$

Encrypt-and-MAC (E&M)

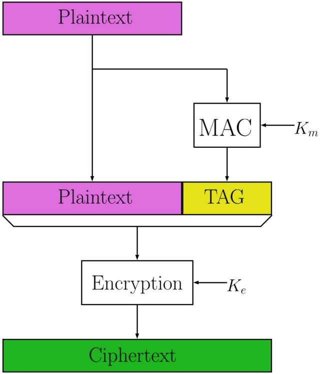
$$\overline{E}(K_e||K_m, M) = E(K_e, M)||T(K_m, M)$$



We can compute $E(K_e, M)$ and $T(K_m, M)$ in parallel.
The SSH protocol is implementing this construction.

MAC-then-Encrypt (MtE)

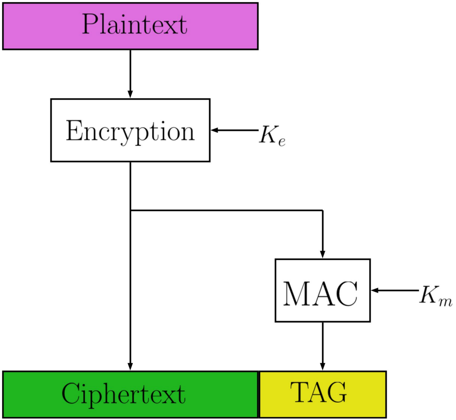
$$\overline{E}(K_e||K_m, M) = E(K_e, M||T(K_m, M))$$



The MAC is encrypted, so harder to attack.
SSL/TLS is implementing this construction.

Encrypt-then-MAC (EtM)

$\overline{E}(K_e||K_m, M) = C||T(K_m, C)$ where $C = E(K_e, M)$



We calculate the MAC of the ciphertext, not the plaintext.
EtM is implemented in IPSec.

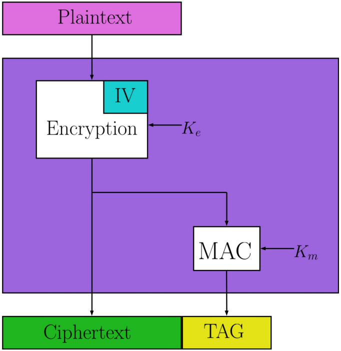
Security of M&E, MtE and EtM

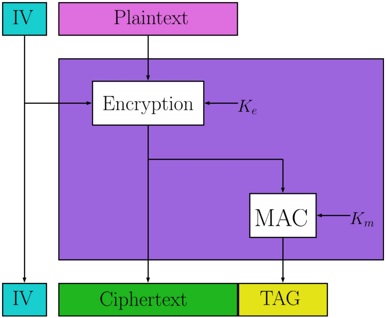
Bellare and Namprempre, 2000

- M&E: MAC can leak information about the message.
- MtE: We can create a new valid ciphertext if the encryption is malleable.
- EtM: Proven secure if the encryption and the MAC are secure.

Is that the end?

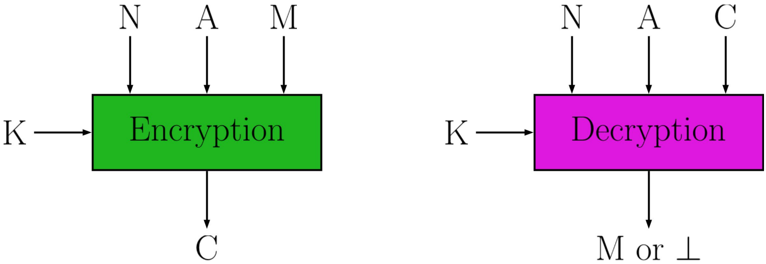
Real schemes do not match. We use a nonce or an initialization vector (IV) external to the schemes.





nAE scheme

$E_K^{N,A}(M) = C$ and $D_K^{N,A}(C) = M$ or $\perp$.



N: Nonce
A: Associated data
K: Secret key
M: Message
C: Ciphertext

nAE properties

Required properties:

- Correctness: if $E_K^{N,A}(M) = C \neq \perp$ then $D_K^{N,A}(C) = M$
- Tidiness: if $D_K^{N,A}(C) = M \neq \perp$ then $E_K^{N,A}(M) = C$

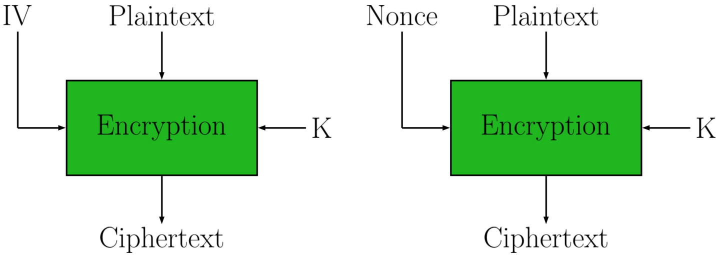
Security properties:

- The encryption output is indistinguishable from random strings in a chosen plaintext attack, the adversary must not repeat nonces.
- The adversary is unable to produce a new valid ciphertext given an encryption oracle. Again, the adversary must not repeat nonces.

nE and ivE

Encryption can be either nonce-based (nE) or IV-based (ivE).

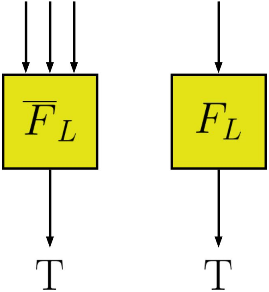
- IV: random initialization vector.
- Nonce: unique initialization vector.



Abstraction of the MAC

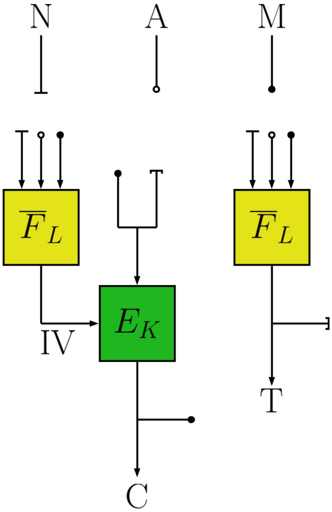
To simplify, we can abstract the MAC as a pseudo-random function.

- vecMAC: A MAC primitive that takes multiple values for its input (here, 3 maximum).
- strMAC: classic MAC as we know.



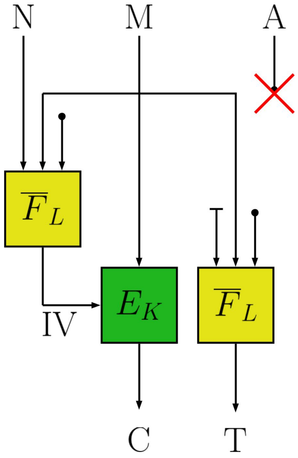
Combinations

Start by creating a basic model and enumerate all possibilities.
There are 160 possible combinations.



Method

Eliminate bad schemes by finding trivial attacks.

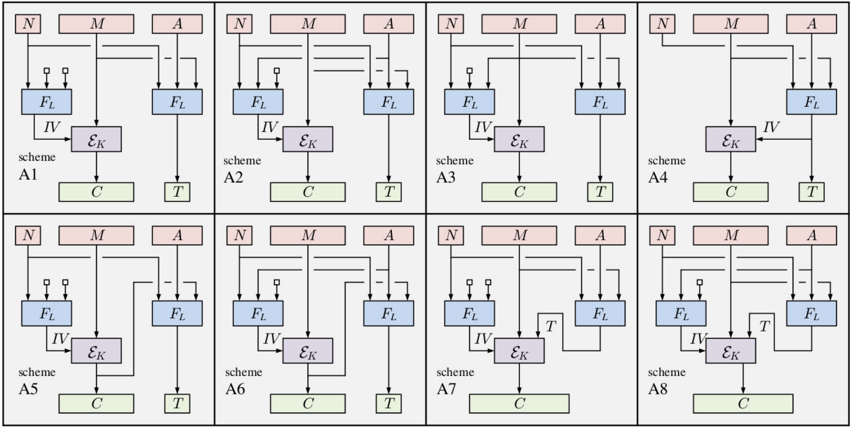


The remaining schemes were analyzed by hand.

A* Schemes

There were 160 candidates, 8 of them are favored (A1-A8), one has a weaker security bound (A9) and three are elusive (A10-A12).

Scheme	IV	Tag	Comment
A1	$F_L^{iv}(N, \sqcup, \sqcup)$	$F_L^{tag}(N, A, M)$	C,T done in parallel
A2	$F_L^{iv}(N, A, \sqcup)$	$F_L^{tag}(N, A, M)$	C,T done in parallel
A3	$F_L^{iv}(N, \sqcup, M)$	$F_L^{tag}(N, A, M)$	Assume IV is recoverable, untruncatable
A4	$F_L^{iv}(N, A, M)$	$F_L^{tag}(N, A, M)$	$F^{iv} = F^{tag}$, untruncatable, nonce-reuse secure
A5	$F_L^{iv}(N, \sqcup, \sqcup)$	$F_L^{tag}(N, A, C)$	M,T done in parallel
A6	$F_L^{iv}(N, A, \sqcup)$	$F_L^{tag}(N, A, C)$	M,T done in parallel
A7	$F_L^{iv}(N, \sqcup, \sqcup)$	$F_L^{tag}(N, A, M)$	Untruncatable
A8	$F_L^{iv}(N, A, \sqcup)$	$F_L^{tag}(N, A, M)$	Untruncatable
A9	$F_L^{iv}(N, A, \sqcup)$	$F_L^{tag}(N, \sqcup, M)$	Weaker bound, untruncatable
A10	$F_L^{iv}(N, A, \sqcup)$	$F_L^{tag}(\sqcup, A, M)$	Security unresolved
A11	$F_L^{iv}(N, A, \sqcup)$	$F_L^{tag}(\sqcup, \sqcup, M)$	Security unresolved
A12	$F_L^{iv}(N, \sqcup, \sqcup)$	$F_L^{tag}(\sqcup, A, M)$	Security unresolved



A1 to A3 is similar to E&M
A4 is SIV mode.
A5 and A6 is EtM.
A7 and A8 is MtE.

Image: Namprempre and al., *Reconsidering generic composition*

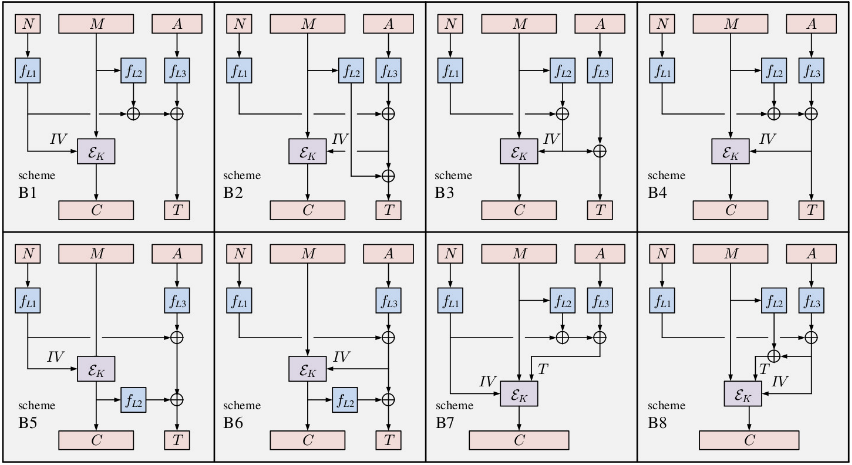
From strMAC to vecMAC

vecMAC is an abstract function, we need something concrete.
Use a *three-xor construction*.

$$F_{L1,L2,L3}(N, A, M) = f'_{L1}(N) \oplus f'_{L2}(A) \oplus f'_{L3}(M)$$

This transformation works for the eight A schemes and is proven secure. We now obtain the B schemes.

B Schemes



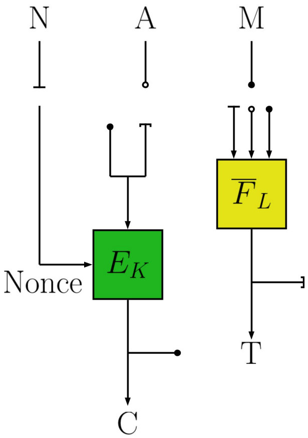
B1 is EAX mode.

Image: Namprempre and al., *Reconsidering generic composition*

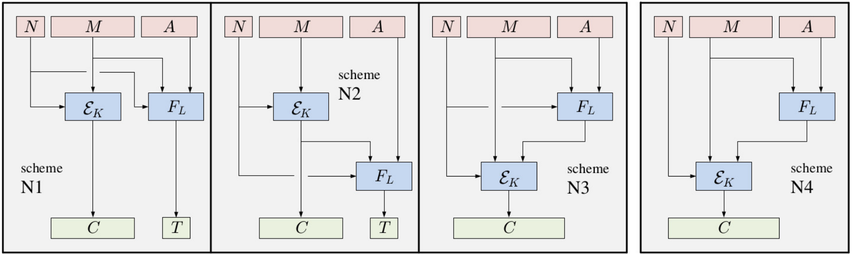
N Schemes

Another model with 20 candidates, three are favored and one is elusive.

We can again use the *three-xor construction*, but we keep the simplicity of vecMAC.



N Schemes



N1 can compute C and T in parallel.
N2 can compute M and T in parallel.
N3 is untruncatable.
N4 has an unresolved security, and C is untruncatable.

Image: Namprempre and al., *Reconsidering generic composition*

ISO 19772

Defines GCM, CCM and EAX very well, but EtM is poorly done.

- Usage of a Starting Value (SV). Unclear if it's a nonce or an IV.
- SV communication is not specified.
- What to do in case of a padding error?

We do not know if it's a scheme built from a pE, or from an ivE.

Conclusion

- Be careful when composing with cryptographic primitives. Additivity is not guaranteed.
- Interpreting cryptography and security results is not trivial. ISO 19772 is a pure example.
- The new result shown here is more concrete and applicable for real cryptography work.

Questions and Remarks?

References

Namprempre, Chanathip and Rogaway, Phillip and Shrimpton, Thomas *Reconsidering generic composition*, Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2014

Bellare, Mihir and Namprempre, Chanathip, *Authenticated encryption: Relations among notions and analysis of the generic composition paradigm*, International Conference on the Theory and Application of Cryptology and Information Security, 2000

Ferguson, Niels and Schneier, Bruce and Kohno, Tadayoshi, *Cryptography Engineering: Design Principles and Practical Applications*, Wiley Publishing, Inc., 2010

ISO/IEC 19772, *Information technology - Security techniques - Authenticated encryption*, 2009

Martin Meredith, *Facepalm*, Birmingham, August 25, 2011