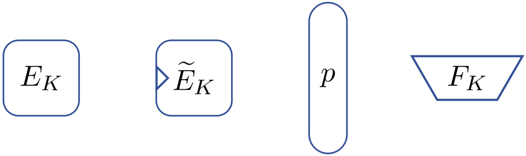
The Limited Power of Verification Queries in Message Authentication and Authenticated Encryption

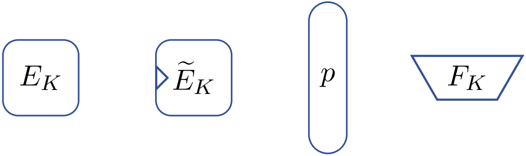
September 29, 2015

Atul Luykx, Bart Preneel, Kan Yasuda

Modes of Operation

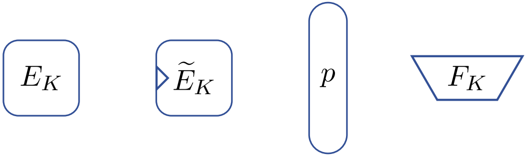


Modes of Operation



Example: AES-OTR Deoxys ASCON OMD

Modes of Operation



Example: AES-OTR Deoxys ASCON OMD

Advantage of modes: able to focus on primitive

1. Reduce security of AE scheme to that of underlying primitive
2. For AE this is done for confidentiality and authenticity

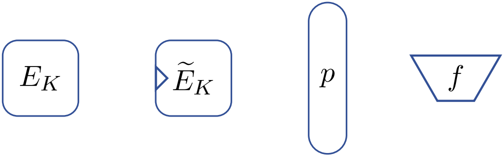
Reduction Loss

1. Reduction is often not perfect, results in a loss of security
2. Loss of security quantified in terms of parameters

Table: Examples of parameters.

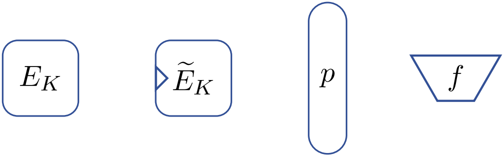
n	Block size
q	Number of tagging or encryption queries
k	Key length
ℓ	Maximum message length
σ	Total number of encryption *and* decryption blocks

Various AE Bounds



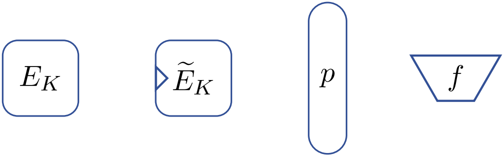
Example: AES-OTR Deoxys ASCON OMD

Various AE Bounds



Example:	AES-OTR	Deoxys	ASCON	OMD
Confidentiality:	$\frac{\sigma^2}{2^n}$ + (S)PRP	0	$\frac{\sigma^2}{2^n}$	$\frac{\sigma^2}{2^n}$ + PRF

Various AE Bounds



Example:	AES-OTR	Deoxys	ASCON	OMD
Confidentiality:	$\frac{\sigma^2}{2^n} + \text{(S)PRP}$	0	$\frac{\sigma^2}{2^n}$	$\frac{\sigma^2}{2^n} + \text{PRF}$
Authenticity:	$+\frac{v}{2^n}$	$+\frac{v}{2^n}$	$+\frac{v}{2^n}$	$+\frac{v}{2^n}$

Improved Bounds: MAC Message Length

Much research performed reducing message length dependence from quadratic to linear for MACs: PMAC, CBC-MAC, EMAC, OMAC, TMAC

$$\frac{\ell^2 q^2}{2^n} \longrightarrow \frac{\ell q^2}{2^n}$$

Improved Bounds: MAC Message Length

Much research performed reducing message length dependence from quadratic to linear for MACs: PMAC, CBC-MAC, EMAC, OMAC, TMAC

$$\frac{\ell^2 q^2}{2^n} \longrightarrow \frac{\ell q^2}{2^n}$$

$n = 128, q = 2^{48}$:

$$\ell \leq 2^{15} \longrightarrow \ell \leq 2^{30}$$

Improved Bounds: MAC Message Length

Much research performed reducing message length dependence from quadratic to linear for MACs: PMAC, CBC-MAC, EMAC, OMAC, TMAC

$$\frac{\ell^2 q^2}{2^n} \longrightarrow \frac{\ell q^2}{2^n}$$

$n = 128, q = 2^{48}$:

$$\ell \leq 2^{15} \longrightarrow \ell \leq 2^{30}$$

$n = 128, \ell = 2^{15}$:

$$q \leq 2^{48} \longrightarrow q \leq 2^{63}$$

Improved Bounds: Permutation Based Modes

	c	n	k	security
Ascon	192	128	96	96
	256	64	128	128
ICEPOLE	254	1026	128	128
	318	962	256	256
NORX	192	320	128	128
	384	640	256	256
GIBBON/ HANUMAN	159	41	80	80
	239	41	120	120

Improved Bounds: Permutation Based Modes

	c	n	k	security
Ascon	96	224	96	96
	128	192	128	128
ICEPOLE	254	1026	128	128
	318	962	256	256
NORX	192	320	128	128
	384	640	256	256
GIBBON/ HANUMAN	159	41	80	80
	239	41	120	120

Improved Bounds: Permutation Based Modes

	c	n	$\frac{n}{n_{\mathrm{old}}}$	k	security
Ascon	96	224	1.75	96	96
	128	192	3	128	128
ICEPOLE	254	1026		128	128
	318	962		256	256
NORX	192	320		128	128
	384	640		256	256
GIBBON/ HANUMAN	159	41		80	80
	239	41		120	120

Improved Bounds: Permutation Based Modes

	c	n	$\frac{n}{n_{\text{old}}}$	k	security
Ascon	96	224	1.75	96	96
	128	192	3	128	128
ICEPOLE	128	1152	1.12	128	128
	256	1024	1.06	256	256
NORX	128	384	1.2	128	128
	256	768	1.2	256	256
GIBBON/ HANUMAN	80	120	2.92	80	80
	120	160	3.90	120	120

Improved security bounds leads to

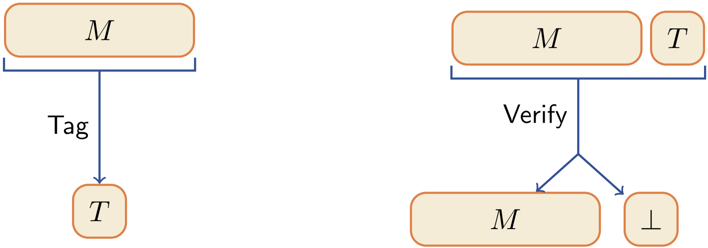
1. Better parameter choices
2. Increased longevity
3. Increased efficiency

Improved security bounds leads to

1. Better parameter choices
2. Increased longevity
3. Increased efficiency

Despite advances, there is still a lot of work left.

Authenticity Definition



$\mathsf{Auth}(q, v)$: forgery success with q tagging queries and v forgery attempts

Authenticity Bounds

$$\frac{\sigma^2}{2^n} \longrightarrow \frac{\ell^2(q + {\color{red}v})^2}{2^n}$$

Authenticity Bounds

$$\frac{\sigma^2}{2^n} \longrightarrow \frac{\ell^2(q+v)^2}{2^n}$$

1. 128 bit block cipher

$$\frac{\ell^2(q+v)^2}{2^{128}}$$

Authenticity Bounds

$$\frac{\sigma^2}{2^n} \longrightarrow \frac{\ell^2(q+v)^2}{2^n}$$

1. 128 bit block cipher
2. Only one-block verification queries

$$\frac{1^2(0+v)^2}{2^{128}}$$

Authenticity Bounds

$$\frac{\sigma^2}{2^n} \longrightarrow \frac{\ell^2(q+v)^2}{2^n}$$

1. 128 bit block cipher
2. Only one-block verification queries

$$\frac{v^2}{2^{128}}$$

Authenticity Bounds

$$\frac{\sigma^2}{2^n} \longrightarrow \frac{\ell^2(q+v)^2}{2^n}$$

1. 128 bit block cipher
2. Only one-block verification queries

$$\frac{v^2}{2^{128}} \quad \text{vs} \quad \frac{v}{2^{128}}$$

Authenticity Bounds

$$\frac{\sigma^2}{2^n} \longrightarrow \frac{\ell^2(q+{\color{red}v})^2}{2^n}$$

1. 128 bit block cipher
2. Only one-block verification queries

$$\frac{v^2}{2^{128}} \quad \text{vs} \quad \frac{v}{2^{128}}$$

$$v = 2^{64}: \quad 1 \quad \text{vs} \quad \frac{1}{2^{64}}$$

Optimal Bound

So far only certain types of MACs have optimal bound:

1. Nonce-based
2. Multiple keys

Excludes PMAC, CBC-MAC, OMAC

Optimal Bound

So far only certain types of MACs have optimal bound:

1. Nonce-based
2. Multiple keys

Excludes PMAC, CBC-MAC, OMAC

For AE

1. except for TBC modes, none with optimal bounds
2. Generic composition: reduction to MAC-security
   $\rightarrow$ need optimal MACs

Question

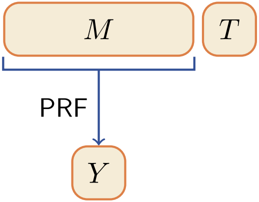
Why do well-designed schemes exhibit quadratic dependence?

Question

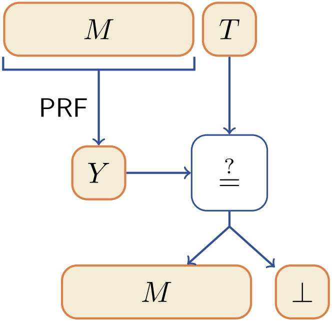
Why do well-designed schemes exhibit quadratic dependence?

Proof techniques

PRF-based MAC



PRF-based MAC



Generic Reduction

Best possible generic reduction:

$$\mathsf{Auth}(q, v)$$

Generic Reduction

Best possible generic reduction:

$$\mathsf{Auth}(q, v) \leq \frac{v}{2^\tau} + \mathsf{PRF}(q + v)$$

Generic Reduction

Best possible generic reduction:

$$\mathsf{Auth}(q, v) \leq \frac{v}{2^\tau} + \mathsf{PRF}(q + v)$$

$$\mathsf{PRF}(q + v) \in \Omega\left(\frac{q^2 + v^2}{2^s}\right)$$

Generic Reduction

Best possible generic reduction:

$$\mathsf{Auth}(q, v) \leq \frac{v}{2^\tau} + \mathsf{PRF}(q + v)$$

$$\mathsf{PRF}(q + v) \in \Omega\left(\frac{q^2 + v^2}{2^s}\right)$$

PMAC

$$\frac{v}{2^\tau} + c \cdot \frac{\ell(q + v)^2}{2^n}$$

PRP-PRF Switch

PRP-PRF Switch: $\dfrac{0.5\sigma^2}{2^n}$

PRP-PRF Switch

PRP-PRF Switch: $\dfrac{0.5\sigma^2}{2^n}$

GCM with nonce length fixed to 96 bits

PRP-PRF Switch

PRP-PRF Switch: $\dfrac{0.5\sigma^2}{2^n}$

GCM with nonce length fixed to 96 bits

Confidentiality:

$$\underbrace{\frac{0.5(\sigma + q + 1)^2}{2^n}}_{\text{PRP-PRF switch}}$$

PRP-PRF Switch

PRP-PRF Switch: $\dfrac{0.5\sigma^2}{2^n}$

GCM with nonce length fixed to 96 bits

Confidentiality:

$$\underbrace{\frac{0.5(\sigma+q+1)^2}{2^n}}_{\text{PRP-PRF switch}}$$

Authenticity:

$$\underbrace{\frac{0.5(\sigma+q+v+1)^2}{2^n}}_{\text{PRP-PRF switch}}+\frac{v(\ell+1)}{2^\tau}$$

Summary

1. Better security bounds improve longevity and efficiency of schemes

Summary

1. Better security bounds improve longevity and efficiency of schemes
2. Many schemes exhibit a quadratic dependence on verification queries

Summary

1. Better security bounds improve longevity and efficiency of schemes
2. Many schemes exhibit a quadratic dependence on verification queries

Conjecture: All CAESAR modes provably achieve the optimal bound.

Summary

1. Better security bounds improve longevity and efficiency of schemes
2. Many schemes exhibit a quadratic dependence on verification queries

Conjecture: All CAESAR modes provably achieve the optimal bound.

Paper in the works

1. Generalizing known techniques, applied to GCM to recover bound
2. Analyze block cipher based modes in detail, applied to PMAC to recover bound