The Design Space of Lightweight Cryptography

Nicky Mouha

[1]ESAT/COSIC, KU Leuven and iMinds, Belgium
[2]Project-team SECRET, Inria, France

NIST Lightweight Cryptography Workshop
July 20, 2015

Lightweight Cryptography

What is Lightweight Cryptography?

- “Lightweight” vs “conventional” crypto
- Should not mean weak crypto

Lightweight Cryptography

What is Lightweight Cryptography?

- “Lightweight” vs “conventional” crypto
- Should not mean weak crypto

Focus on Three Topics

- Lightweight crypto is much more!

Lightweight Cryptography

What is Lightweight Cryptography?

- "Lightweight" vs "conventional" crypto
- Should not mean weak crypto

Focus on Three Topics

- Lightweight crypto is much more!

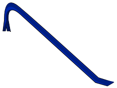
Main Focus: Symmetric-Key Crypto

- Maybe insights for other domains?

Three Topics

How to Measure Security

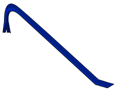
- Attack models
- Key, block and tag sizes



Three Topics

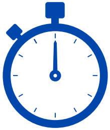
How to Measure Security

- Attack models
- Key, block and tag sizes



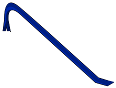
How to Measure Efficiency

- "Theoretical" vs "actual" efficiency
- Scaling law for symmetric-key crypto



Three Topics

How to Measure Security

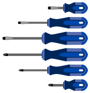


- Attack models
- Key, block and tag sizes

How to Measure Efficiency

- "Theoretical" vs "actual" efficiency
- Scaling law for symmetric-key crypto

Picking the Right Tool for the Job



- Analyzing lightweight requirements
- Often wrong choices at protocol level!

How to Measure Security: Motivation

Short Keys: Sometimes Okay?

How to Measure Security: Motivation

Short Keys: Sometimes Okay?

- *"The key is changed every half hour".*

How to Measure Security: Motivation

Short Keys: Sometimes Okay?

- *"The key is changed every half hour".*
- *"The data is not worth a million dollars".*

How to Measure Security: Motivation

Short Keys: Sometimes Okay?

- *"The key is changed every half hour".*
- *"The data is not worth a million dollars".*

Statements: Often Heard, Seldom Refuted

How to Measure Security: Motivation

Cell Phone Communication

- GSM
- A5/1 algorithm
- Key: 64 bits

How to Measure Security: Motivation

Cell Phone Communication

- GSM
- A5/1 algorithm
- Key: 64 bits

Nohl et al.

- Large precomputation (dozens of GPU years)
- Table of 1.6 TB
- Break in ≈ 5 s on commodity hardware
- Data complexity: one 114-bit GSM burst

Information-Theoretic Framework

Information-Theoretic Framework

- Deterministic algorithms $\rightarrow$ statistical objects
- Output: unknown until *queried*
- Computationally-unbounded adversaries

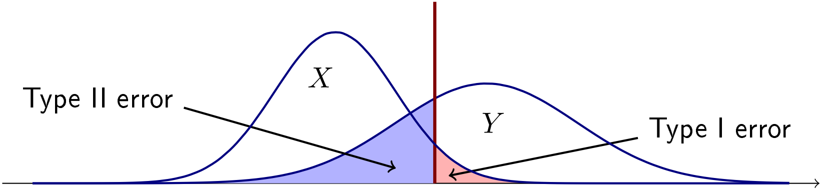
Information-Theoretic Framework

Information-Theoretic Framework

- Deterministic algorithms → statistical objects
- Output: unknown until *queried*
- Computationally-unbounded adversaries

Hypothesis Test

- Distinguish between “real world” and “ideal world”

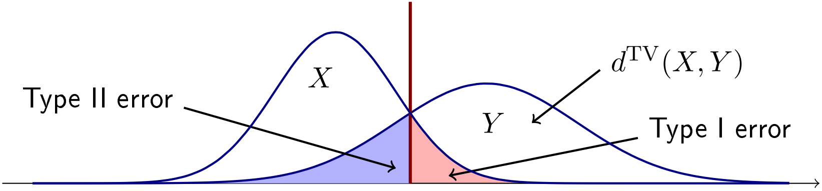


Information-Theoretic Framework

- Deterministic algorithms $\rightarrow$ statistical objects
- Output: unknown until *queried*
- Computationally-unbounded adversaries

Hypothesis Test $\rightarrow$ Total Variation Distance

- Distinguish between "real world" and "ideal world"



Information-Theoretic Framework

Example (Asiacrypt '14)

Let $\mathbf{D}$ be PA1-adversary for APE, $\mathbf{E}$ be plaintext extractor

$$\mathsf{PA1}^{\mathbf{E}}_{\mathsf{APE}}(\mathbf{D}) \leq \frac{\sigma^2}{2^{r+c}} + \frac{2\sigma(\sigma+1)}{2^c}$$

(σ: total # blocks of all queries, r: rate, c: capacity)

Information-Theoretic Framework

Example (Asiacrypt '14)

Let $\mathbf{D}$ be PA1-adversary for APE, $\mathbf{E}$ be plaintext extractor

$$\mathsf{PA1}^{\mathbf{E}}_{\mathsf{APE}}(\mathbf{D}) \leq \frac{\sigma^2}{2^{r+c}} + \frac{2\sigma(\sigma+1)}{2^c}$$

(σ: total # blocks of all queries, r: rate, c: capacity)

Interpretation

- Upper bound on success probability of any attack
- "Secure up to about $\sigma = 2^{c/2}$ blocks"

Information-Theoretic Framework

Types of Queries

- Data complexity (D): access to device under attack
  (under *any* key?)
- Time complexity (T): knowledge of the algorithm
  (Kerckhoffs's principle)

Information-Theoretic Framework

Types of Queries

- Data complexity (D): access to device under attack (under *any* key?)
- Time complexity (T): knowledge of the algorithm (Kerckhoffs's principle)
- Attacks with rekeying: often overlooked (CRYPTO '15)

Information-Theoretic Framework

Types of Queries

- Data complexity (D): access to device under attack
  (under *any* key?)
- Time complexity (T): knowledge of the algorithm
  (Kerckhoffs's principle)
- Attacks with rekeying: often overlooked (CRYPTO '15)

Do Not Use:

- Short keys: see earlier (GSM)
- Short blocks: degrades security of mode of operation
- Short tags: tag guessing (works regardless of rekeying!)

How to Measure Efficiency

Examples of Efficiency Metrics

- # modular exponentiations
- # block cipher calls / plaintext block
- # permutation calls / message block

How to Measure Efficiency

Examples of Efficiency Metrics

- # modular exponentiations
- # block cipher calls / plaintext block
- # permutation calls / message block

Scaling Law

- More refined metric for symmetric-key crypto
- Better understanding of lightweight

Scaling Law

"When the input size of a symmetric-key primitive doubles, the number of operations (roughly) doubles as well".

Scaling Law

"When the input size of a symmetric-key primitive doubles, the number of operations (roughly) doubles as well".

Remarks

- Not intuitive: $b \to b$ bits: $(2^b)^{2^b} = 2^{b2^b}$ functions
- Not rigorous: based on design choices and attacks
- How to count "operations"?

Scaling Law

"When the input size of a symmetric-key primitive doubles, the number of operations (roughly) doubles as well".

Remarks

- Not intuitive: $b \to b$ bits: $(2^b)^{2^b} = 2^{b2^b}$ functions
- Not rigorous: based on design choices and attacks
- How to count "operations"?

Next Slides: Scaling Law Examples

Scaling Law: Fixed Word Size

PHOTON: 4-bit Words

- 100/144/196/256-bit permutation: 12 rounds
- (288-bit permutation: 12 rounds, but 8-bit word size)

Scaling Law: Fixed Word Size

PHOTON: 4-bit Words

- 100/144/196/256-bit permutation: 12 rounds
- (288-bit permutation: 12 rounds, but 8-bit word size)

Rijndael (256-bit key): 8-bit Words

- 128/192/256-bit block size: 14 rounds

Scaling Law: Fixed Word Size

PHOTON: 4-bit Words

- 100/144/196/256-bit permutation: 12 rounds
- (288-bit permutation: 12 rounds, but 8-bit word size)

Rijndael (256-bit key): 8-bit Words

- 128/192/256-bit block size: 14 rounds

Skein: 64-bit Words

- 256/512-bit block/key size: 72 rounds
- 1024-bit block/key size: 80 rounds
- Overdesign? Best (non-biclique) attack is on 36 rounds (Yu et al., SAC '13)

Scaling Law: Variable Word Size

BLAKE

- 960-to-256-bit: 14 rounds (32-bit words)
- 1920-to-512-bit: 16 rounds (64-bit words)

Scaling Law: Variable Word Size

BLAKE

- 960-to-256-bit: 14 rounds (32-bit words)
- 1920-to-512-bit: 16 rounds (64-bit words)

SHA-2

- SHA-256: 768-to-256-bit: 64 rounds (32-bit words)
- SHA-512: 1536-to-512 bit: 80 rounds (64-bit words)

Scaling Law: Variable Word Size

BLAKE

- 960-to-256-bit: 14 rounds (32-bit words)
- 1920-to-512-bit: 16 rounds (64-bit words)

SHA-2

- SHA-256: 768-to-256-bit: 64 rounds (32-bit words)
- SHA-512: 1536-to-512 bit: 80 rounds (64-bit words)

Keccak

- 800-bit permutation: 22 rounds (32-bit words)
- 1600-bit permutation: 24 rounds (64-bit words)
- Note: zero-sum distinguisher for full-round 1600-bit permutation (Boura et al., Duan-Lai)

Scaling Law: Counterexamples?

Grøstl

- 512-bit permutation: 10 rounds
- 1024-bit permutation: 14 rounds

Scaling Law: Counterexamples?

Grøstl

- 512-bit permutation: 10 rounds
- 1024-bit permutation: 14 rounds
- If 15 rounds: three n-bit or one $2n$-bit: same cost

Scaling Law: Counterexamples?

Grøstl

- 512-bit permutation: 10 rounds
- 1024-bit permutation: 14 rounds
- If 15 rounds: three n-bit or one $2n$-bit: same cost
- Best attacks: resp. 9/10 rounds (Jean et al., FSE '12)

Scaling Law: Counterexamples?

Grøstl

- 512-bit permutation: 10 rounds
- 1024-bit permutation: 14 rounds
- If 15 rounds: three n-bit or one $2n$-bit: same cost
- Best attacks: resp. 9/10 rounds (Jean et al., FSE '12)

Spongent

- b-bit permutation, $r = b/2$ rounds, $b/4$ S-boxes/round: $b^2/8$ S-boxes in total

Scaling Law: Counterexamples?

Grøstl

- 512-bit permutation: 10 rounds
- 1024-bit permutation: 14 rounds
- If 15 rounds: three n-bit or one $2n$-bit: same cost
- Best attacks: resp. 9/10 rounds (Jean et al., FSE '12)

Spongent

- b-bit permutation, $r = b/2$ rounds, $b/4$ S-boxes/round: $b^2/8$ S-boxes in total
- Four n-bit or one $2n$-bit permutation: same cost

Scaling Law: Counterexamples?

Grøstl

- 512-bit permutation: 10 rounds
- 1024-bit permutation: 14 rounds
- If 15 rounds: three n-bit or one $2n$-bit: same cost
- Best attacks: resp. 9/10 rounds (Jean et al., FSE '12)

Spongent

- b-bit permutation, $r = b/2$ rounds, $b/4$ S-boxes/round: $b^2/8$ S-boxes in total
- Four n-bit or one $2n$-bit permutation: same cost
- 272-bit Spongent: 5x lower throughput than 256-bit PHOTON (Bogdanov et al., IEEE Trans. Comp. 2013)

Picking the Right Tool for the Job

Targets

- Hardware area or code size, RAM, ROM
- Latency, throughput, power and/or energy
- Secure implementation!

Picking the Right Tool for the Job

Targets

- Hardware area or code size, RAM, ROM
- Latency, throughput, power and/or energy
- Secure implementation!

Considerations

- Collision resistance needed?
- Ciphertext expansion? Computation vs communication
- Misuse resistance?

Picking the Right Tool for the Job

Targets

- Hardware area or code size, RAM, ROM
- Latency, throughput, power and/or energy
- Secure implementation!

Considerations

- Collision resistance needed?
- Ciphertext expansion? Computation vs communication
- Misuse resistance?

Goal of Lightweight Crypto

- When standard solutions fail to satisfy constraints
- Not less secure, but using new academic insights
- Most widely usable algorithm that satisfies all constraints

Conclusion

What is Lightweight Cryptography?

- Not "weak crypto"
- Do not use short key/block/tag sizes

Conclusion

What is Lightweight Cryptography?

- Not "weak crypto"
- Do not use short key/block/tag sizes

Focus on Three Topics

- Security model: T and D queries, rekeying
- Scaling law: data doubles: computation doubles
- Match algorithm with application

Conclusion

What is Lightweight Cryptography?

- Not “weak crypto”
- Do not use short key/block/tag sizes

Focus on Three Topics

- Security model: T and D queries, rekeying
- Scaling law: data doubles: computation doubles
- Match algorithm with application

Questions?