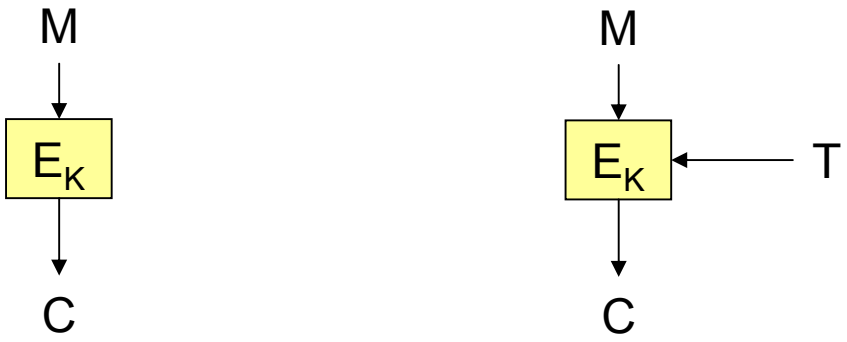
Improved Security Analysis of XEX and LRW modes

Kazuhiko Minematsu

NEC Corp.

Introduction

- Tweakable Block Ciphers [LRW02]
  - Block ciphers with additional parameter "tweak"
  - Tweak is public, and provides variability
    - two different tweaks give two instances of non-tweakable block cipher.

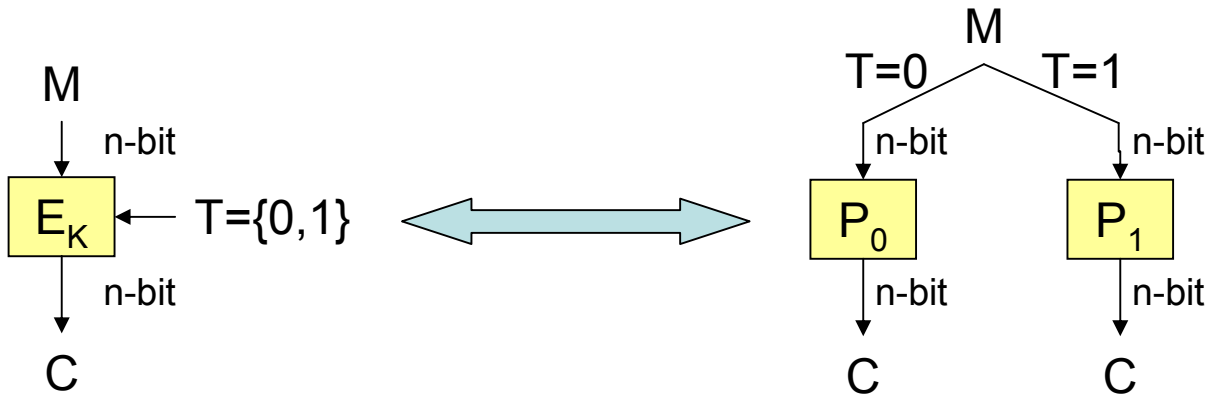


Applications of TWBC

- Use tweak as public randomizer
  - In disk-sector encryption, we use sector number as tweak
- Key component of some advanced modes of operation
  - Authenticated encryption (e.g., OCB)
  - MAC (e.g., PMAC, OMAC)
  - and more!

Requirements of TWBC

- Efficient. Changing a tweak should be fast (faster than changing a key)
- Secure. Indistinguishable from the family of uniform random permutations (URPs)
- Our focus: strong TWBC = secure against CPCA + chosen tweak (we simply call it CCA)



P_i is the uniform random permutation (URP)

Constructions of strong TWBC

- Designed from scratch
  - Ex. HPC and Mercy
- Mode of operation: turn a CCA-secure block cipher into a strong TWBC
  - LRW mode by Liskov et al. [LRW02]: first proposal of strong TWBC
  - XEX mode by Rogaway [R03]: “optimized” LRW for building advanced modes

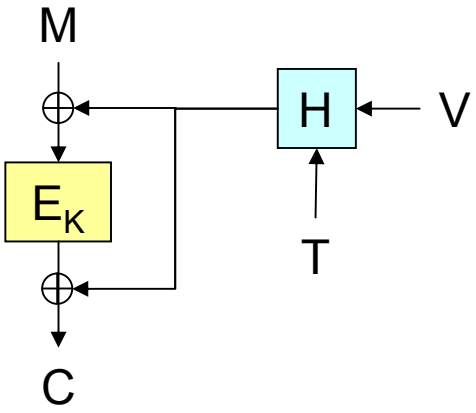
Our contributions

- A general construction for strong TWBC from CCA-secure BC
  - including LRW and XEX
  - useful for building “one-key” TWBC
- Using our construction, we provide:
  - improved security proofs for XEX and LRW
  - improvements to LRW

The LRW mode

- Mask-Enc-Mask with offset function H
  - H(V,*) : ε-Almost XOR universal (AXU) hash function (V is the key)

    Def. $\Pr(H(V,t) \oplus H(V,t') = c) \leq \epsilon \quad \text{for any } t \neq t' \text{ and } c$
- Inherently two-key: K must be independent of V



LRW mode

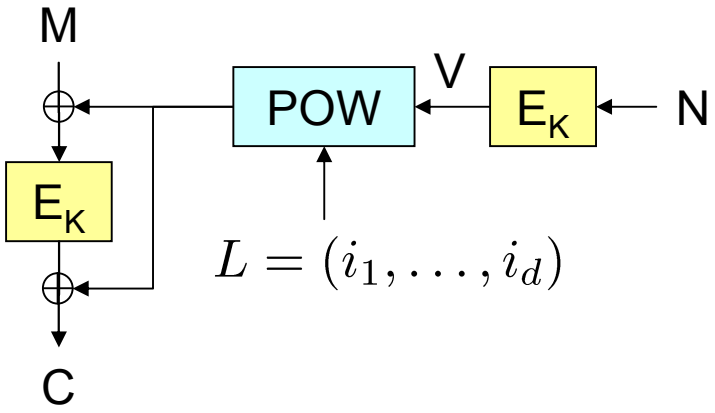
plaintext M

ciphertext C

tweak T

The XEX mode

- Reduce two-key to one-key
- Using powering-up construction
  - $\mathrm{POW}(\underbrace{i_1, \ldots, i_d}_{\text{index vector}}, V) = \prod_{j=1}^{d} \alpha_j^{i_j} \cdot V$ (basis: α_j)
  - Incremental tweak update (w.r.t. index) w/ very small cost



XEX mode

plaintext M

ciphertext C

tweak T=(N,L)

Allowed parameter setting

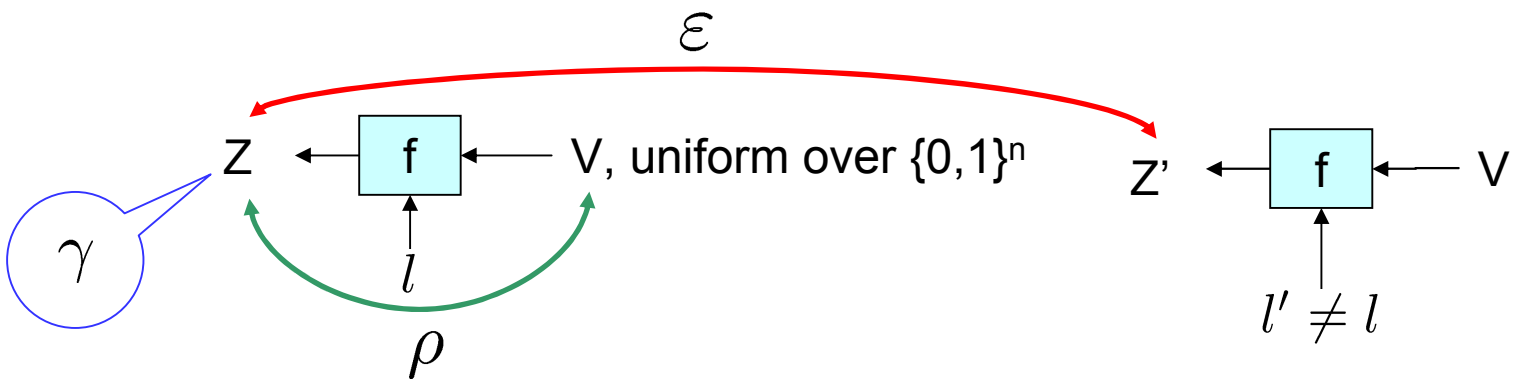
- (From [R03]) To make XEX secure, basis and index vectors must:
  - provide unique representations
    - $\prod_{j=1}^{d} \alpha_j^{i_j} \neq \prod_{j=1}^{d} \alpha_j^{i'_j}$ for any $(i_1, \ldots, i_d) \neq (i'_1, \ldots, i'_d)$
  - exclude all-zero index vector
    - $\prod_{j=1}^{d} \alpha_j^{i_j} \neq 1$ (identity element in GF(2^n))
      - If not, a simple CCA-attack is possible

Why these conditions?

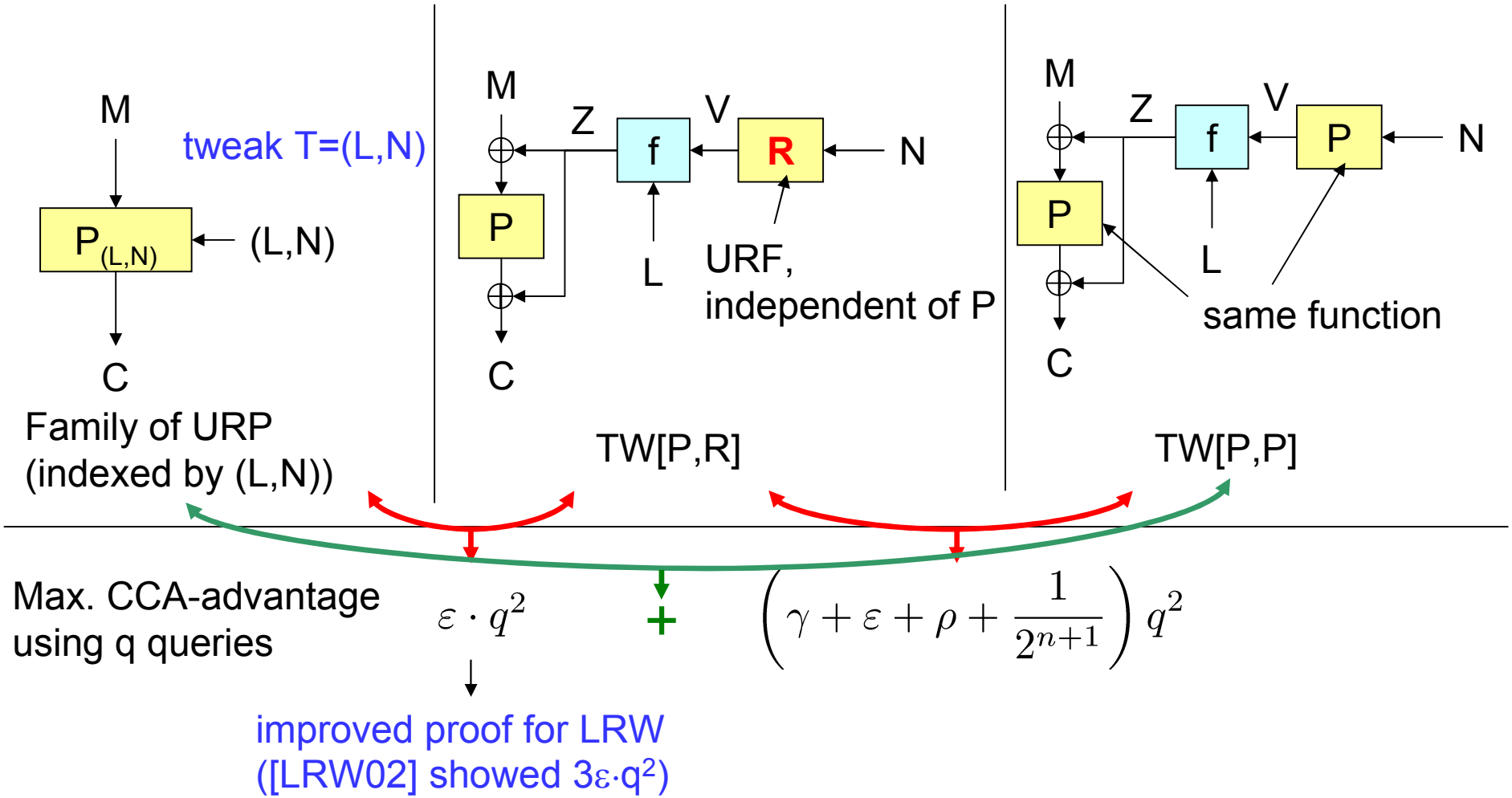
We explain the reason in a general setting

Our result

- For $f : \mathcal{L} \times \{0,1\}^n \to \{0,1\}^n$, let γ, ε, and ρ be defined as:
  - $\max_{l \in \{0,1\}^n, c \in \{0,1\}^n} \Pr(f(l,V) = c) \leq \gamma$
  - $\max_{l,l' \in \mathcal{L}, l \neq l', c \in \{0,1\}^n} \Pr(f(l,V) \oplus f(l',V) = c) \leq \varepsilon \quad (\varepsilon\text{-AXU})$
  - $\max_{l \in \mathcal{L}, c \in \{0,1\}^n} \Pr(f(l,V) \oplus V = c) \leq \rho$



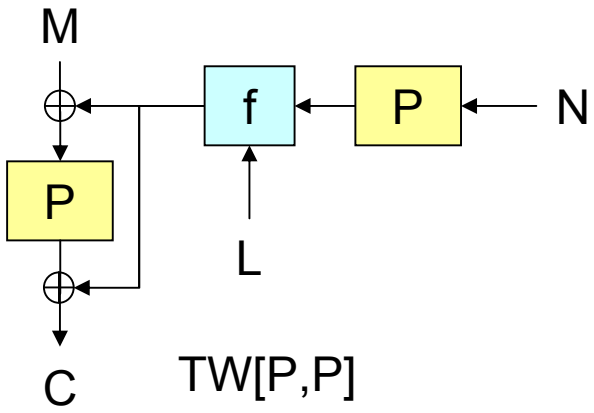
Our result


M
tweak T=(L,N)
P(L,N)
(L,N)
C
Family of URP
(indexed by (L,N))
M
Z
f
V
R
N
P
L
URF,
independent of P
C
TW[P,R]
M
Z
f
V
P
N
P
L
same function
C
TW[P,P]
Max. CCA-advantage
using q queries
$\varepsilon \cdot q^2$
+
$\left(\gamma + \varepsilon + \rho + \frac{1}{2^{n+1}}\right) q^2$
improved proof for LRW
([LRW02] showed 3ε·q²)

Our result

- Thus, the max. CCA-adv. of TW[P,P] is:

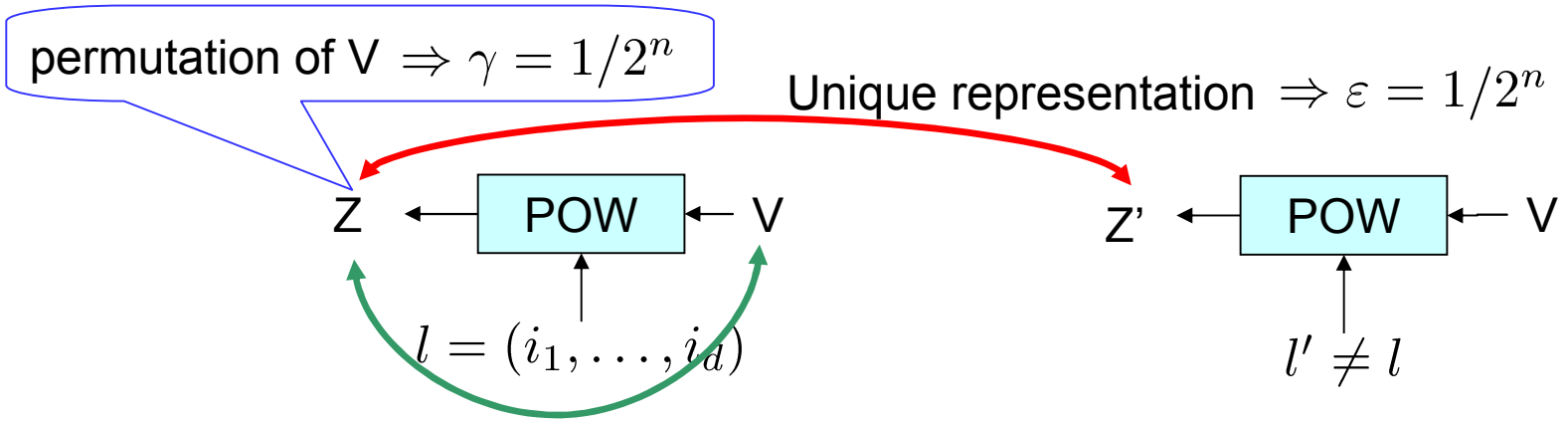
$$\mathbf{Adv}^{\widetilde{\mathbf{sprp}}}_{\mathrm{TW[P,P]}}(q) \leq \left(2\varepsilon + \gamma + \rho + \frac{1}{2^{n+1}}\right) q^2 \qquad \text{(Theorem 4)}$$



  - Computational analog (i.e. use CCA-secure BC instead of URP) is easily derived from this

Proving the security of XEX

- Recall that $\mathrm{POW}(i_1, \ldots, i_d, V) = \prod_{j=1}^{d} \alpha_j^{i_j} \cdot V$



$Z \oplus V$ is a permutation of V $\Rightarrow \rho = 1/2^n$

if L=(0,0,..,0) was allowed, $\rho = 1$

Thus $\gamma = \varepsilon = \rho = 1/2^n$

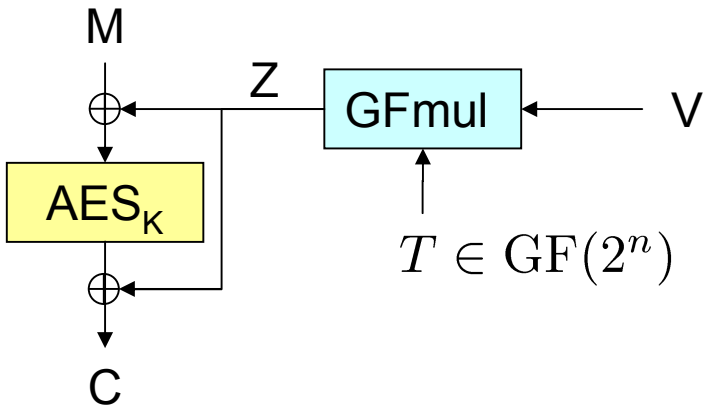
and we have $\mathbf{Adv}^{\widetilde{\mathbf{sprp}}}_{\mathrm{XEX[P]}}(q) \leq \frac{4.5q^2}{2^n}$

On our security proof

- Slightly better than the previous proofs
  - for XEX, [R03] showed 9.5 instead of 4.5
  - for LRW, [LRW02] showed 3ε instead of ε
- Key idea: Maurer's methodology [M02]
  - sometimes gives tighter bound than other methods (ex. the case of 3-round Feistel)
- General one-key construction. Not restricted to POW function

Applications of our theorem

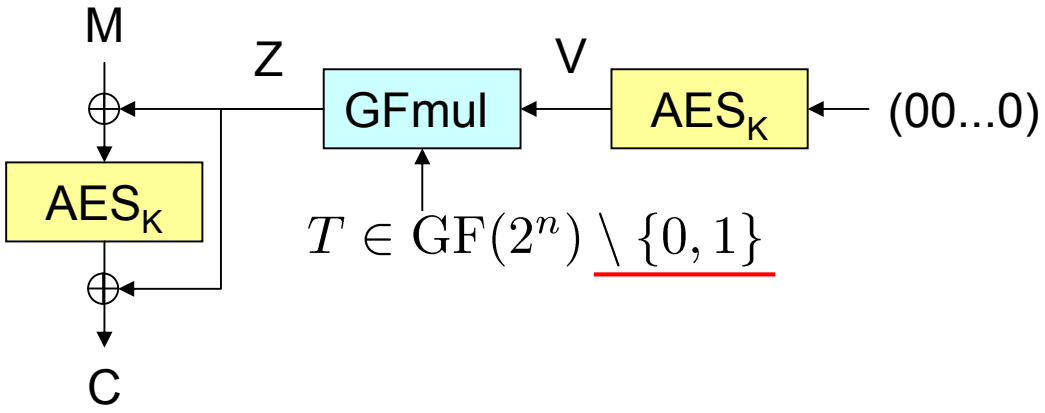
- Various improvements to LRW-AES [IEEE SISWG]
  - LRW-AES: E as AES, offset fnc =GFmul(T,V)
    - One AES key K + one n-bit key V, and n-bit tweak T (n=128)
  - GFmul is $1/2^n$-AXU, thus security bound is 1.0 $q^2/2^n$



(Two-key) LRW-AES

Simple one-key LRW-AES

- Using the same idea as XEX
  - slightly reduced tweak set (excluding zero and identity elements)
- One-key w/o additional computation
- Security bound: $4.5q^2/2^n$ (same as XEX)

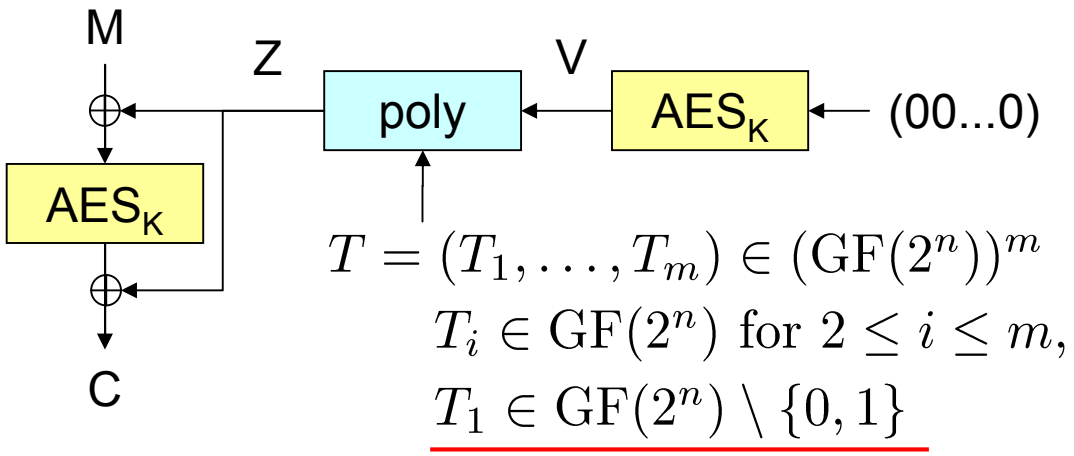


One-key LRW-AES

For a larger tweak set

- Use polynomial-evaluation hash

$$\mathrm{poly}(T, V) = \sum_{i=1}^{m} V^i T_i, \quad T = (T_1, \ldots, T_m)$$



One-key LRW-AES w/ a large tweak set

Proving the security

- Simple fact: a polynomial of deg. m has at most m solutions

$1 \leq \deg(Z) \leq m \Rightarrow \gamma = m/2^n$

if t_1=0 was allowed, deg(Z) could be 0

$1 \leq \deg(Z - Z') \leq m \Rightarrow \varepsilon = m/2^n$

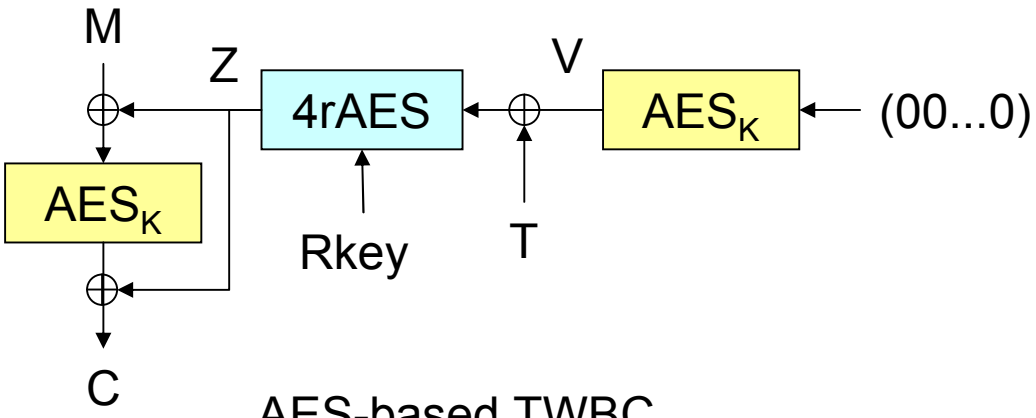
$1 \leq \deg(Z - V) \leq m \Rightarrow \rho = m/2^n$

if t_1=1 was allowed, deg(Z-V) could be 0

$\gamma = \varepsilon = \rho = m/2^n$, thus the security bound is (4m+0.5) $q^2/2^n$

Using a reduced-round AES

- Known fact: 4-round AES has a very good differential property (ex. Keliher and Sui [KS05])
- Use 4-round AES instead of GFmul
  - arbitrarily tweak update at the cost of 4-round AES
- γ , ε, and ρ are similarly defined (by taking account of the Rkey's distribution)



AES-based TWBC

Security analysis

- Let Rkey be 384-bit (2nd to 4th round keys)
  - 1st round key is fixed to any value
- Using a slight extension of our theorem, the AES-based TWBC is provably secure, if Rkey is
  - uniform and independent of AES key
    - Security bound: $(2^{16}+2.5)q^2/2^{128}$ (using [KS05])
  - fixed to (e.g.) all-zero, and if some non-computational assumption about 4rAES holds
    - ε and ρ must be small even if Rkey is fixed to all-zero : (a weak form of) the Hypothesis of stochastic equivalence

Conclusion

- A general (one-key) construction of strong TWBC
  - providing an intuitive and improved proof for XEX (and LRW)
  - efficient one-key versions of LRW-AES
- Future research direction
  - more applications of TWBC
  - TWBC beyond the birthday bound (i.e. $1/2^{n/2}$)

Thank you!

An attack against a flawed XEX