Modes of Operations for Block Ciphers

Debrup Chakraborty

CINVESTAV

email: debrup@cs.cinvestav.mx

To be covered : Lecture 2

- OCB
- AEAD
- CMC and EME
- PEP, HCTR

Finite Fields

- Let $GF(2^n)$ denote the field with 2^n elements.
- Let F^* denotes the multiplicative subgroup in $GF(2^n)$
- We can view a point in $GF(2^n)$ in any of the following ways:
  - An abstract point in the field
  - A n bit string $a_{n-1}a_{n-2}\ldots a_0$, where $a_i \in \{0,1\}$
  - As a formal polynomial $a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots a_1 x + a_0$ with binary coefficients
  - As a number between 0 and $2^n - 1$

Finite Fields (Contd.)

For example the string $0^{125}101$, can be considered as

- As a 128 bit string
- A point in the field $GF(2^{128})$
- As the polynomial $x^2 + 1$
- As the number 5

Finite Fields (Contd.)

- To add two elements in $GF(2^n)$, we just take the bitwise XOR of the two elements
- To multiply, we fix a suitable (sparse) irreducible polynomial and multiply modulo that polynomial
- If we consider a primitive polynomial in place of an irreducible one then x generates all points in F^*.

Tweakable Block Ciphers

- Tweakable blockciphers takes in an additional input other than the message and the key.
- This additional input is called tweak
- The tweak is a non-secret quantity
- This notion was first formalized by Liskov, Rivest and Wagner [LRW]
- The purpose behind tweaks was to increase variability of the cipher texts.
- Tweakable block ciphers were also used for designing modes of operations by [LRW], but they were inefficient

Powering up constructions

- Rogaway suggested some efficient construction of tweakable blockciphers
- He calls them as powering up constructions
- These block-ciphers were efficiently used to instantiate modes of operations and MAC algorithms.
- These constructions are simple, efficient and above all they are easy to analyze.

The XEX construction

- Assume the field to be represented as a primitive polynomial
- Then the elements $1, x, x^2, x^3, \ldots, x^{2^n-2}$ are all distinct
- Given a block cipher E_K, define the tweakable blockcipher as

$$\tilde{E}_K^{N,i}(M) = E_K(M \oplus \Delta) \oplus \Delta,$$

$$\text{where } \; \Delta = x^i \mathcal{N} \; \text{ and } \; \mathcal{N} = E_K(N)$$

- Here the tweak space is

$$\mathcal{T} = [0, 1, \ldots, 2^n - 2] \times \{0, 1\}^n$$

The General XEX construction

- Given a block cipher E_K, define the tweakable blockcipher as

$$\tilde{E}_K^{N,i_1,i_2,\ldots,i_k}(M) = E_K(M \oplus \Delta) \oplus \Delta,$$

where $\Delta = \alpha_1^{i_1}\alpha_2^{i_2}\ldots\alpha_k^{i_k}\mathcal{N}$ and $\mathcal{N} = E_K(N)$

- Here the tweak space is

$$\mathcal{T} = I_i \times I_2 \times \ldots I_k \times \{0,1\}^n$$

- Each α_i is an element in the group $F_{2^n}^*$
- The α_is should provide **unique representation**

The XEX construction

Unique representation

- Fix a group G. The choice of parameters for XEX construction is a list of bases $\alpha_1^{i_1}, \alpha_2^{i_2}, \ldots \alpha_k^{i_k} \in G$ and a set $I_i \times I_2 \times \ldots I_k$ of allowed indices, where each I_i is a set of integers. We say that the choice of parameters allows unique representation if for any $(i_1, i_2, \ldots i_k), (j_1, j_2, \ldots j_k) \in I_i \times I_2 \times \ldots I_k$ we have that

$$\alpha_1^{i_1} \alpha_2^{i_2} \ldots \alpha_k^{i_k} = \alpha_1^{j_1} \alpha_2^{j_2} \ldots \alpha_k^{j_k}$$

implies

$$(i_1, i_2, \ldots i_k) = (j_1, j_2, \ldots j_k)$$

The XEX Construction

Allowed bases

- It can be shown that, for the group $F^*_{2^{128}}$ the following bases provides unique representations
  - Base x with allowed indices $[0, \ldots, 2^{126}]$
  - Bases x and $1 + x$ with allowed indices $[0, \ldots, 2^{115}] \times [0, \ldots, 2^{10}]$
  - Base x, $1 + x$ and $1 + x + x^2$ with allowed indices $[0, \ldots, 2^{44}] \times [0, \ldots, 2^7 \times [0, \ldots, 2^7$
- In fact a more strong result can be proved, but this would be enough for our purpose.

The XEX Construction

The security of XEX construction

- Define $\tilde{E} : \mathcal{K} \times (\{0,1\}^n \times I_1 \times I_2 \times \ldots \times I_K) \times \{0,1\}^n \to \{0,1\}^n$ by $\tilde{E}_K^{N,i_1,i_2,\ldots,i_k}(M) = E_K(M \oplus \Delta) \oplus \Delta$ where $\Delta = \alpha_1^{i_1}\alpha_2^{i_2}\ldots\alpha_k^{i_k}\mathcal{N}$ and $\mathcal{N} = E_K(N)$. Then

$$\mathrm{Adv}_{\tilde{E}_K}^{\pm p\tilde{r}p}(t,q) \leq \mathrm{Adv}_{E_K}^{\pm prp}(t',2q) + \frac{4.5q^2}{2^n}$$

- In other words $\tilde{E}_K$ is a SPRP if E_K is an SPRP

The OCB1