Tools for Symmetric Key Provable Security

Mridul Nandi

Indian Statistical Institute, Kolkata

ASK Workshop, Changsha
10 Dec. 2017

Outline of the talk

1. Probability in Cryptography
   - Well Known Distribution in Cryptography
   - Some Metrics on Probability Distributions
2. Two Tools: H-Coefficient and χ^2
   - H-Coefficient Technique
   - Mirror theory
   - χ^2 Method
3. Some Constructions and Applications
   - Encrypted Davies-Meyer (EDM) Construction
   - Truncation Construction
   - Sum of Permutations Construction

Outline of the talk

1. Probability in Cryptography
   - Well Known Distribution in Cryptography
   - Some Metrics on Probability Distributions
2. Two Tools: H-Coefficient and χ^2
   - H-Coefficient Technique
   - Mirror theory
   - χ^2 Method
3. Some Constructions and Applications
   - Encrypted Davies-Meyer (EDM) Construction
   - Truncation Construction
   - Sum of Permutations Construction

Outline of the talk

1. Probability in Cryptography
   - Well Known Distribution in Cryptography
   - Some Metrics on Probability Distributions
2. Two Tools: H-Coefficient and χ^2
   - H-Coefficient Technique
   - Mirror theory
   - χ^2 Method
3. Some Constructions and Applications
   - Encrypted Davies-Meyer (EDM) Construction
   - Truncation Construction
   - Sum of Permutations Construction

Notations for Probability

1. $X \leftarrow \Omega$: X is a random variable with sample space Ω.
2. $\Pr_X$ denotes the *probability function* of X.
3. For an *event* $E \subseteq \Omega$ we denote the probability of the event E realized by X as
$$\Pr_X(E) \text{ or } \Pr(X \in E)$$
4. $\Pr_X(E \mid F)$ is the **conditional probability** defined only when $\Pr_X(F)$ is positive and it is defined as
$$\Pr_X(E \cap F) / \Pr_X(F).$$

Notations for Probability

1. $x^t := (x_1, \ldots, x_t)$ for any positive t.
   $X^t := (X_1, \ldots, X_t) \leftarrow \Omega = \Omega_1 \times \cdots \times \Omega_t$ is also called joint random variable.
2. We denote $\Pr(X_i = x_i \mid X^{i-1} = x^{i-1})$ as $\Pr_X(x_i \mid x^{i-1})$.
3. Let $X \leftarrow \Omega$, $f : \Omega \to \mathbb{R}$ then

$$\mathbf{Ex}(f(X)) = \sum_{x \in \Omega} f(x) \Pr_X(x).$$

4. If X is a real valued random variable

$$\mathbf{Var}(X) = E((X - \mathbf{Ex}(X))^2).$$

Notations for Probability

1. $x^t := (x_1, \ldots, x_t)$ for any positive t.
   $X^t := (X_1, \ldots, X_t) \leftarrow \Omega = \Omega_1 \times \cdots \times \Omega_t$ is also called joint random variable.
2. We denote $\Pr(X_i = x_i \mid X^{i-1} = x^{i-1})$ as $\Pr_X(x_i \mid x^{i-1})$.
3. Let $X \leftarrow \Omega$, $f : \Omega \to \mathbb{R}$ then

$$\mathbf{Ex}(f(X)) = \sum_{x \in \Omega} f(x) \Pr_X(x).$$

4. If X is a real valued random variable

$$\mathbf{Var}(X) = E((X - \mathbf{Ex}(X))^2).$$

With and Without Replacement Sample

1. **Examples.** In statistics with replacement (WR) and without replacement sample (WOR) sampling are very popular.
2. $\mathsf{U} := (U_1, \ldots, U_t) \leftarrow_{\mathrm{wr}} \mathcal{S}$ says that $\mathsf{U} \leftarrow_{\$} \mathcal{S}^t$. So we specify $\Pr_{\mathsf{U}}$ completely as $\Pr_{\mathsf{U}}(x^t) = |\mathcal{S}|^{-t}$.
3. WOR sample $\mathsf{V} := (V_1, \ldots, V_t) \leftarrow_{\mathrm{wor}} \mathcal{S}$ is specified through conditional probability as

$$\Pr_{\mathsf{V}}(x_i \mid x^{i-1}) = \frac{1}{|\mathcal{S}|-i+1}, \text{ for all distinct } x_1, \ldots, x_i \in \mathcal{S}.$$

With and Without Replacement Sample

1. **Examples**. In statistics with replacement (WR) and without replacement sample (WOR) sampling are very popular.

2. $\mathsf{U} := (U_1, \ldots, U_t) \leftarrow_{\text{wr}} \mathcal{S}$ says that $\mathsf{U} \leftarrow_{\$} \mathcal{S}^t$. So we specify $\Pr_{\mathsf{U}}$ completely as $\Pr_{\mathsf{U}}(x^t) = |\mathcal{S}|^{-t}$.

3. WOR sample $\mathsf{V} := (V_1, \ldots, V_t) \leftarrow_{\text{wor}} \mathcal{S}$ is specified through conditional probability as

$$\Pr_{\mathsf{V}}(x_i \mid x^{i-1}) = \frac{1}{|\mathcal{S}|-i+1}, \text{ for all distinct } x_1, \ldots, x_i \in \mathcal{S}.$$

Why do we study WR and WOR in Cryptography?

1. Let $f \leftarrow_{\$} \mathsf{Func}(D, R)$ (random function). Then, for any distinct $x_1, \ldots, x_q \in D$,

$$(f(x_1), \ldots, f(x_q)) \leftarrow_{\text{wr}} R.$$

2. If $\pi \leftarrow_{\$} \mathsf{Perm}(R)$ (random permutation - we use it for block cipher or permutation in the ideal model) then

$$(\pi(x_1), \ldots, \pi(x_q)) \leftarrow_{\text{wor}} R.$$

3. The both results are true even if x_i's are some functions of y^{i-1} where $y_j = f(x_j)$ (or $y_j = \pi(x_j)$). This happens for adaptive adversary interacting with f or π.

Why do we study WR and WOR in Cryptography?

1. Let $f \leftarrow_{\$} \mathsf{Func}(D, R)$ (random function). Then, for any distinct $x_1, \ldots, x_q \in D$,

$$(f(x_1), \ldots, f(x_q)) \leftarrow_{\text{wr}} R.$$

2. If $\pi \leftarrow_{\$} \mathsf{Perm}(R)$ (random permutation - we use it for block cipher or permutation in the ideal model) then

$$(\pi(x_1), \ldots, \pi(x_q)) \leftarrow_{\text{wor}} R.$$

3. The both results are true even if x_i's are some functions of y^{i-1} where $y_j = f(x_j)$ (or $y_j = \pi(x_j)$). This happens for adaptive adversary interacting with f or π.

Why do we study WR and WOR in Cryptography?

1. Let $f \leftarrow_\$ \mathsf{Func}(D, R)$ (random function). Then, for any distinct $x_1, \ldots, x_q \in D$,

$$(f(x_1), \ldots, f(x_q)) \leftarrow_{\text{wr}} R.$$

2. If $\pi \leftarrow_\$ \mathsf{Perm}(R)$ (random permutation - we use it for block cipher or permutation in the ideal model) then

$$(\pi(x_1), \ldots, \pi(x_q)) \leftarrow_{\text{wor}} R.$$

3. The both results are true even if x_i's are some functions of y^{i-1} where $y_j = f(x_j)$ (or $y_j = \pi(x_j)$). This happens for adaptive adversary interacting with f or π.

Why do we study WR and WOR in Cryptography?

1. In cryptography blockcipher modeled to be pseudorandom permutation.
2. This means (using hybrid argument) that we can replace random permutation instead of a blockcipher.
3. Consider the XOR construction: $E_K(x\|0) \oplus E_K(x\|1)$.
4. If we replace blockcipher by random permutation, te output distribution of the XOR construction is same as X^t where

$$X_1 = V_1 \oplus V_2, \ldots, X_t = V_{2t-1} \oplus V_{2t}$$

and

$$(V_1, \ldots, V_t) \leftarrow_{\text{wor}} \{0,1\}^n.$$

Why do we study WR and WOR in Cryptography?

1. In cryptography blockcipher modeled to be pseudorandom permutation.
2. This means (using hybrid argument) that we can replace random permutation instead of a blockcipher.
3. Consider the XOR construction: $E_K(x\|0) \oplus E_K(x\|1)$.
4. If we replace blockcipher by random permutation, te output distribution of the XOR construction is same as X^t where

$$X_1 = V_1 \oplus V_2, \ldots, X_t = V_{2t-1} \oplus V_{2t}$$

and

$$(V_1, \ldots, V_t) \leftarrow_{\text{wor}} \{0,1\}^n.$$

Outline of the talk

1. Probability in Cryptography
   - Well Known Distribution in Cryptography
   - Some Metrics on Probability Distributions
2. Two Tools: H-Coefficient and χ^2
   - H-Coefficient Technique
   - Mirror theory
   - χ^2 Method
3. Some Constructions and Applications
   - Encrypted Davies-Meyer (EDM) Construction
   - Truncation Construction
   - Sum of Permutations Construction

Total variation

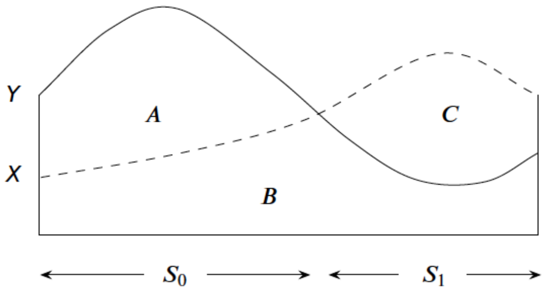
Definition

Total variation (or statistical distance) is a metric on the set of probability functions over Ω.

$$\|P_0 - P_1\| = \frac{1}{2} \sum_{x \in \Omega} |P_0(x) - P_1(x)|.$$

Geometric interpretation of Total variation

Total variation between X and Y = area $A+$ area C.
(Picture courtesy Shoup's book "A Computational Introduction to Number Theory and Algebra").



Indistinguishability Game and total variation

- $\mathcal{A}$ is a distinguisher - two oracles $\mathcal{O}_1$ and $\mathcal{O}_2$.
- The *advantage* of the adversary in this game, denoted $\mathsf{Adv}_{\mathcal{A}}(\mathcal{O}_1, \mathcal{O}_2)$, is given by

$$\mathsf{Adv}^{\text{dist}}_{\mathcal{O}_1,\mathcal{O}_2}(\mathcal{A}) := |\Pr(\mathcal{A}^{\mathcal{O}_1} \to 1) - \Pr(\mathcal{A}^{\mathcal{O}_2} \to 1)|,$$

- If X^q and Y^q denote the outputs of $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively. Then,

$$\mathsf{Adv}^{\text{dist}}_{\mathcal{O}_1,\mathcal{O}_2}(\mathcal{A}) \leq \| \Pr_{X^q} - \Pr_{Y^q} \|.$$

Properties of Total variation

1. $\|P_0 - P_1\| \leq 1$. When equality holds?
2. **Triangle inequality**. Let P_i be the probability function of X_i, $i \in [d] \stackrel{\text{def}}{=} \{1, 2, \ldots, d\}$ then

$$\|P_1 - P_d\| \leq \|P_1 - P_2\| + \cdots + \|P_{d-1} - P_d\|.$$

Some Examples of Total Variation

We sometimes denote $d_{\mathrm{TV}}(X, Y) = \| \Pr_X - \Pr_Y \|$.

1. Let $\mathcal{T} \subseteq \mathcal{S}$ and $X \leftarrow_{\$} \mathcal{S}, Y \leftarrow_{\$} \mathcal{T}$. Then,

$$d_{\mathrm{TV}}(X, Y) = 1 - \frac{|\mathcal{T}|}{|\mathcal{S}|}.$$

2. Let $|\mathcal{S}| = N$, $U^q \leftarrow_{\mathrm{wr}} \mathcal{S}$ and $V^q \leftarrow_{\mathrm{wor}} \mathcal{S}$ then

$$d_{\mathrm{TV}}(U, V) = 1 - \prod_{i=1}^{q-1}(1 - \frac{i}{N}) = cp(q, N)$$

where $cp(q, N)$ denotes the collision probability of q random elements chosen from a set of size N.

Chi-square distance

The χ^2 distance between $\mathbf{P_0}$ and $\mathbf{P_1}$, with $\mathbf{P_0} \ll \mathbf{P_1}$ (support of $\mathbf{P_0}$ is contained in that of $\mathbf{P_1}$), is defined as

$$d_{\chi^2}(\mathbf{P_0}, \mathbf{P_1}) := \sum_{x \in \Omega} \frac{(\mathbf{P_0}(x) - \mathbf{P_1}(x))^2}{\mathbf{P_1}(x)}.$$

- Has its origin in mathematical statistics dating back to Pearson.
- It can be seen that χ^2 distance is not symmetric, does not satisfy triangle inequality.

Chi-square distance

The χ^2 distance between $\mathbf{P_0}$ and $\mathbf{P_1}$, with $\mathbf{P_0} \ll \mathbf{P_1}$ (support of $\mathbf{P_0}$ is contained in that of $\mathbf{P_1}$), is defined as

$$d_{\chi^2}(\mathbf{P_0}, \mathbf{P_1}) := \sum_{x \in \Omega} \frac{(\mathbf{P_0}(x) - \mathbf{P_1}(x))^2}{\mathbf{P_1}(x)}.$$

- Has its origin in mathematical statistics dating back to Pearson.
- It can be seen that χ^2 distance is not symmetric, does not satisfy triangle inequality.

Other Metrics

1. Helinger distance: Steinberger used this metric to bound advantage of key-alternating cipher.
2. Renyi divergence of order a (generalized form of χ^2. When $a = 2$ it is closely related to χ^2). Used in lattice based cryptography.
3. Separation measurement (used in Markov chain).
4. KL divergence is popular in cryptography. Also used in the proof of the χ^2 method.

Outline of the talk

1. Probability in Cryptography
   - Well Known Distribution in Cryptography
   - Some Metrics on Probability Distributions
2. Two Tools: H-Coefficient and χ^2
   - H-Coefficient Technique
   - Mirror theory
   - χ^2 Method
3. Some Constructions and Applications
   - Encrypted Davies-Meyer (EDM) Construction
   - Truncation Construction
   - Sum of Permutations Construction

Outline of the talk

1. Probability in Cryptography
   - Well Known Distribution in Cryptography
   - Some Metrics on Probability Distributions
2. Two Tools: H-Coefficient and χ^2
   - H-Coefficient Technique
   - Mirror theory
   - χ^2 Method
3. Some Constructions and Applications
   - Encrypted Davies-Meyer (EDM) Construction
   - Truncation Construction
   - Sum of Permutations Construction

1. $\mathcal{O}_1$ or $\mathcal{O}_2$ two oracles returning $\mathcal{Y}$ elements.
2. Transcript: $y^q \in \mathcal{Y}^q$.
3. Let X^q and Y^q be the responses while $\mathcal{A}$ interacts with $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively.

Theorem of H-coefficient technique

Theorem (H-coefficient technique)

Let $\mathcal{Y}^q = \mathcal{V}_{\text{good}} \sqcup \mathcal{V}_{\text{bad}}$ *be a partition. Suppose for any* $x^q \in \mathcal{V}_{\text{good}}$,

$$\frac{\Pr(X^q = x^q)}{\Pr(Y^q = x^q)} := \frac{\mathsf{ip}_{\text{real}}}{\mathsf{ip}_{\text{ideal}}} \geq 1 - \epsilon_{\text{ratio}},$$

and

$$\Pr[Y^q \in \mathcal{V}_{\text{bad}}] \leq \epsilon_{\text{bad}}.$$

Then,

$$\mathsf{Adv}^{\text{dist}}_{\mathcal{O}_1,\mathcal{O}_2}(\mathcal{A}) \leq \epsilon_{\text{ratio}} + \epsilon_{\text{bad}}.$$

Simple Applications

1. PRP-PRF switching lemma.
2. Hash-then-PRF.
3. Hash-then-TBC.
4. Many more...

Summing up H-Coefficient

1. Good tool for birthday bound.
2. Some times we have beyond birthday bound, mostly $2^{3n/4}$ and $2^{2n/3}$ (in case of xor of k permutations we have bound of the form $2^{(2k-1)n/2k}$).
3. Not so powerful for optimal security (i.e., n bit security).
4. Mirror theory for sum of permutation. Not easy to understand the proof. Seems to have non-trivial gaps.

Outline of the talk

1. Probability in Cryptography
   - Well Known Distribution in Cryptography
   - Some Metrics on Probability Distributions
2. Two Tools: H-Coefficient and χ^2
   - H-Coefficient Technique
   - Mirror theory
   - χ^2 Method
3. Some Constructions and Applications
   - Encrypted Davies-Meyer (EDM) Construction
   - Truncation Construction
   - Sum of Permutations Construction

What is Mirror theory?

1. A combinatorial result.
2. Hall's result: Let $\mathcal{G}$ be an abelian group and $f : \mathcal{G} \to \mathcal{G}$ be a function such that $\sum_{x \in \mathcal{G}} f(x) = 0$. Then there exists two permutations π_1, π_2 over $\mathcal{G}$ such that $f = \pi_1 - \pi_2$.
3. It has been proved by induction by Marshall J. Hall in 1951.

What is Mirror theory?

1. Patarin extend this with a cryptographic motivation.
2. Number of functions is N^N and the number of permutations is $N!$ where $N = |\mathcal{G}|$.
3. The number of pairs of permutations (π_1, π_2) such that $f = \pi_1 - \pi_2$ is about $\frac{N!^2}{N^N}$ (on the average).
4. Instead of matching a function exactly, match over a domain of size q (the query set for an adversary).

What is Mirror theory?

1. Patarin claimed for $q < N/67$ and for any q-distinct x^q, and any (not necessarily distinct) $y_1, \ldots, y_q$ (so no bad transcripts and hence $\epsilon_{\text{bad}} = 0$),

$$\#\{(\pi_1, \pi_2) : \ \pi_1(x_i) + \pi_2(x_i) = y_i\} \geq \frac{N!^2}{N^q} \times (1 - \epsilon_{\text{ratio}})$$

   where $\epsilon_{\text{ratio}} = O(q/2^n)$

2. In other words,

$$\Pr(\mathsf{RP}_1(x_1) + \mathsf{RP}_2(x_1) = y_1, \ldots, \mathsf{RP}_1(x_q) + \mathsf{RP}_2(x_q) = y_q)$$

$$\geq \frac{1 - \epsilon_{\text{ratio}}}{N^q}.$$

Recall that for coefficients H technique, we need to compute a lower bound for

$$\Pr(X^q = x^q) \geq \frac{1 - \epsilon_{\text{ratio}}}{N^q}.$$

Mirror theory essentially provides the lower bound.

$$\Pr(\mathsf{RP}_1(x_1) + \mathsf{RP}_2(x_1) = y_1, \ldots, \mathsf{RP}_1(x_q) + \mathsf{RP}_2(x_q) = y_q)$$

$$\geq \frac{1 - O(q/N)}{N^q}.$$

Hence, $\mathsf{Adv}^{\text{dist}}_{\mathcal{O}_1,\mathcal{O}_2}(\mathcal{A}) = O(q/N)$.

What is Mirror theory?

1. Similar result with a single permutations.
2. The number of permutations π such that $\pi(0\|x_i) + \pi(1\|x_i) = y_i$ is at least $\frac{N!^2}{N^q}$ for $q < N/67$.
   1. So $\epsilon_{\text{ratio}} = 0$. However, y_i's are non-zero (need a bad set of transcripts and $\epsilon_{\text{bad}} = q/2^n$).
3. In other words, for all q-distinct x^q and non-zero y_i's,

$$\Pr(\mathsf{RP}(0\|x_1)+\mathsf{RP}(1\|x_1) = y_1, \ldots, \mathsf{RP}(0\|x_q)+\mathsf{RP}(1\|x_q) = y_q)$$

$$\geq \frac{1}{N^q}.$$

Patarin considered the following general problem also called mirror theory.

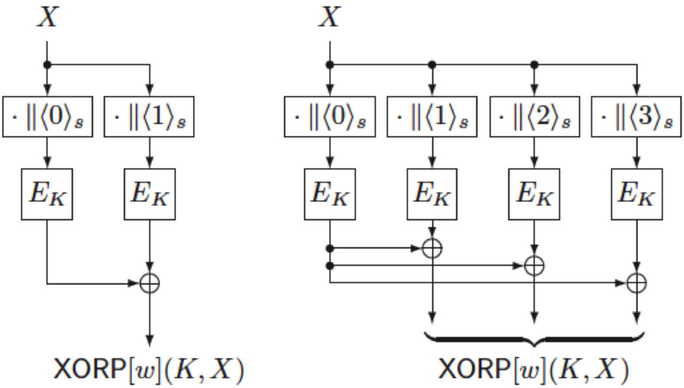
1. distinct $x_{i,j} \in \{0,1\}^n$, $i \in [q], j \in [w]$ and
2. $y_{i,j} \in \{0,1\}^n$. $i \in [q], j \in [w]$ such that $y_{i,j}$'s are nonzero and for every i, $y_{i,1}, \ldots, y_{i,w-1}$ are distinct.

$$\Pr(\text{ for all } i,\ \mathsf{RP}(x_{i,1}) \oplus \mathsf{RP}(x_{i,w}) = y_{i,1}, \ldots,$$
$$\mathsf{RP}(x_{i,w-1}) \oplus \mathsf{RP}(x_{i,w}) = y_{i,w-1}) \geq \frac{1}{N^q}.$$

This is also studied in CENC (by Tetsu Iwata, FSE 2006).

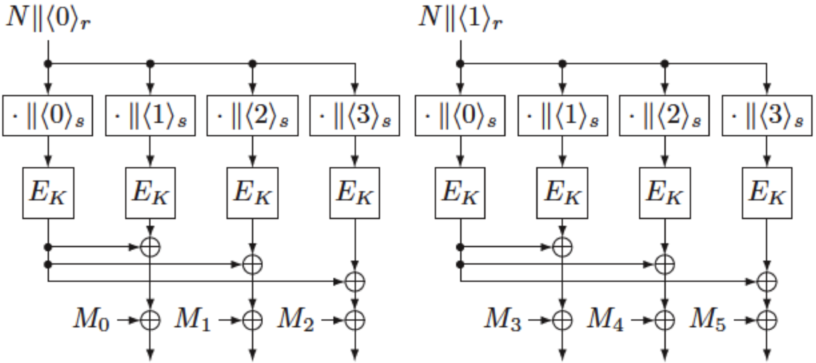
Key stream for CENC with $w = 2$, $w = 4$

(Picture courtesy: https://eprint.iacr.org/2016/1087.pdf).



CENC cipher with $w = 4$

(Picture courtesy: https://eprint.iacr.org/2016/1087.pdf).



Outline of the talk

χ^2 Method

- $\mathsf{X} := (\mathsf{X}_1, \ldots, \mathsf{X}_q)$ and $\mathsf{Y} := (\mathsf{Y}_1, \ldots, \mathsf{Y}_q)$ are two random vectors of size q distributed over Ω^q.
- $$\mathbf{P}_{\mathbf{0}|x^{i-1}}[x_i] = \Pr(\mathsf{X}_i = x_i | \mathsf{X}_1 = x_1, \ldots, \mathsf{X}_{i-1} = x_{i-1})$$
  $$\mathbf{P}_{\mathbf{1}|x^{i-1}}[x_i] = \Pr(\mathsf{Y}_i = x_i | \mathsf{Y}_1 = x_1, \ldots, \mathsf{Y}_{i-1} = x_{i-1})$$
- When $i = 1$, $\mathbf{P}_{\mathbf{0}|x^{i-1}}[x_1]$ represents $\mathbf{P}[\mathsf{X}_1 = x_1]$. Similarly, for $\mathbf{P}_{\mathbf{1}|x^{i-1}}[x_1]$.

- Let $x^{i-1} \in \Omega^{i-1}$, $i \geq 1$.
- $\chi^2(\cdot)$ a real valued function defined as

$$\chi^2(x^{i-1}) := d_{\chi^2}(\mathbf{P}_{\mathbf{0}|x^{i-1}}, \mathbf{P}_{\mathbf{1}|x^{i-1}}).$$

- In other notation,

$$\chi^2(x^{i-1}) := \sum_{x_i} \frac{\left(\Pr_{\mathsf{X}}(x_i|x^{i-1}) - \Pr_{\mathsf{Y}}(x_i|x^{i-1})\right)^2}{\Pr_{\mathsf{Y}}(x_i|x^{i-1})}.$$

- Let $x^{i-1} \in \Omega^{i-1}$, $i \geq 1$.
- $\chi^2(\cdot)$ a real valued function defined as

$$\chi^2(x^{i-1}) := d_{\chi^2}(\mathbf{P}_{\mathbf{0}|x^{i-1}}, \mathbf{P}_{\mathbf{1}|x^{i-1}}).$$

- In other notation,

$$\chi^2(x^{i-1}) := \sum_{x_i} \frac{\left(\Pr_{\mathsf{X}}(x_i|x^{i-1}) - \Pr_{\mathsf{Y}}(x_i|x^{i-1})\right)^2}{\Pr_{\mathsf{Y}}(x_i|x^{i-1})}.$$

Theorem

Suppose $\mathbf{P_0}$ *and* $\mathbf{P_1}$ *denote probability distributions of* $\mathsf{X} := (\mathsf{X}_1, \ldots, \mathsf{X}_q)$ *and* $\mathsf{Y} := (\mathsf{Y}_1, \ldots, \mathsf{Y}_q)$ *and for all* $x_1, \ldots, x_{i-1}$*, we have* $\mathbf{P}_{\mathbf{0}|x^{i-1}} \ll \mathbf{P}_{\mathbf{1}|x^{i-1}}$. *Then*

$$\|\mathbf{P_0} - \mathbf{P_1}\| \leq \left(\frac{1}{2} \sum_{i=1}^{q} \mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})] \right)^{\frac{1}{2}}.$$

Comparison with H-coefficient technique

1. Need: conditional probability instead of joint probabilities.
2. Suppose, for all x^q and $i \leq q$,

$$1 + \epsilon \geq \frac{\Pr_{\mathsf{X}}(x_i | x^{i-1})}{\Pr_{\mathsf{Y}}(x_i | x^{i-1})} \geq 1 - \epsilon$$

3. Then, $\frac{\Pr_{\mathsf{X}}(x^q)}{\Pr_{\mathsf{Y}}(x^q)} \geq 1 - q\epsilon$ and so $\| \Pr_{\mathsf{X}} - \Pr_{\mathsf{Y}} \| \leq \epsilon \times q$.
4. If we apply χ^2 method, $\| \Pr_{\mathsf{X}} - \Pr_{\mathsf{Y}} \| \leq \epsilon \times \sqrt{q/2}$.
5. If we know more on the distributions get better bound.

Switching between PRF and PRP

1. $\Pr_{\mathsf{Y}}(x_i|x^{i-1}) = 1/2^n$ for all i-distinct x^i

$$\Pr_{\mathsf{X}}(x_i|x^{i-1}) = 1/(2^n - i + 1) \qquad \text{if } x_i \notin x^{i-1}$$
$$= 0 \qquad \text{if } x_i \in x^{i-1}$$

2.

$$\frac{\left(\Pr_{\mathsf{X}}(x_i|x^{i-1}) - \Pr_{\mathsf{Y}}(x_i|x^{i-1})\right)^2}{\Pr_{\mathsf{Y}}(x_i|x^{i-1})} = \frac{(i-1)^2}{2^n(2^n - i + 1)^2} \qquad \text{if } x_i \notin x^{i-1}$$
$$= \frac{1}{2^n} \qquad \text{if } x_i \in x^{i-1}$$

Switching between PRF and PRP

1. $\Pr_{\mathsf{Y}}(x_i|x^{i-1}) = 1/2^n$ for all i-distinct x^i

$$\Pr_{\mathsf{X}}(x_i|x^{i-1}) = 1/(2^n - i + 1) \qquad \text{if } x_i \notin x^{i-1}$$
$$= 0 \qquad \text{if } x_i \in x^{i-1}$$

2.

$$\frac{\left(\Pr_{\mathsf{X}}(x_i|x^{i-1}) - \Pr_{\mathsf{Y}}(x_i|x^{i-1})\right)^2}{\Pr_{\mathsf{Y}}(x_i|x^{i-1})} = \frac{(i-1)^2}{2^n(2^n - i + 1)^2} \qquad \text{if } x_i \notin x^{i-1}$$
$$= \frac{1}{2^n} \qquad \text{if } x_i \in x^{i-1}$$

Switching between PRF and PRP

$$\chi^2(x^{i-1}) = \sum_{x_i} \frac{\left(\Pr_{\mathsf{X}}(x_i|x^{i-1}) - \Pr_{\mathsf{Y}}(x_i|x^{i-1})\right)^2}{\Pr_{\mathsf{Y}}(x_i|x^{i-1})}$$
$$= \frac{i-1}{2^n} + \frac{(i-1)^2}{2^n(2^n-i+1)}.$$

By χ^2 method,

$$\| \Pr_{\mathsf{X}} - \Pr_{\mathsf{Y}} \| \leq \sum_{i=1}^{q} \frac{1}{2}(\mathbf{Ex}(\chi^2(\mathsf{X}^{i-1})))^{1/2}$$
$$= \sqrt{\frac{q(q-1)}{2^{n+1}} + \frac{q^3}{2^{2n}}}.$$

Outline of the talk

1. Probability in Cryptography
   - Well Known Distribution in Cryptography
   - Some Metrics on Probability Distributions
2. Two Tools: H-Coefficient and χ^2
   - H-Coefficient Technique
   - Mirror theory
   - χ^2 Method
3. Some Constructions and Applications
   - Encrypted Davies-Meyer (EDM) Construction
   - Truncation Construction
   - Sum of Permutations Construction

Comparisons

Construction	H-coefficient	using mirror Th.	χ^2
EDM	$(q^3/2^{2n})^{1/2}$	$q/2^n$	$(q^4/2^{3n})^{1/2}$
XORP	-	$q/2^n$	$q/2^n$
XORP (2-keyed)	-	$q/2^n$	$q^{1.5}/2^{1.5n}$
Trunc-RP$_m$	$(q/2^{n-\frac{m}{2}})^{\frac{2}{3}}$	-	$q/2^{n-\frac{m}{2}}$

Outline of the talk

1. Probability in Cryptography
   - Well Known Distribution in Cryptography
   - Some Metrics on Probability Distributions
2. Two Tools: H-Coefficient and χ^2
   - H-Coefficient Technique
   - Mirror theory
   - χ^2 Method
3. Some Constructions and Applications
   - Encrypted Davies-Meyer (EDM) Construction
   - Truncation Construction
   - Sum of Permutations Construction

Encrypted Davies-Meyer (EDM) Construction

$\mathsf{EDM}_{\pi,\pi'} : \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}^n$

- Takes two permutations $\pi, \pi' \in \mathsf{Perm}_n$ as key.
- On input $x \in \{0,1\}^n$, returns $\pi'(\pi(x) \oplus x)$.

Bound using coefficients H technique (Cogliati and Seurin - Crypto 2016)

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{EDM}}(\mathcal{A}) \leq \frac{5q^{\frac{3}{2}}}{N}.$$

Bound using χ^2 method (Dai, Hoang, Tessaro - Crypto 2017)

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{EDM}}(\mathcal{A}) \leq \frac{3q^2}{N^{\frac{3}{2}}}.$$

Proof Sketch : $\mathsf{EDM}_{\pi,\pi'}(x) = \pi'(\pi(x) \oplus x)$

upper bd $\Pr_{\mathsf{X}}(x_i|x^{i-1}) \le 1/(2^n - i) \le \frac{1}{2^n} + \frac{2i}{2^{2n}}$.

lower bd $\Pr_{\mathsf{X}}(x_i|x^{i-1}) \ge \frac{2^n - 4i}{2^n(2^n - i)} \ge \frac{1}{2^n} - \frac{4i}{2^{2n}}$.

$$\left| \Pr_{\mathsf{X}}(x_i|x^{i-1}) - \frac{1}{2^n} \right| \le \frac{4i}{2^{2n}}.$$

- $\chi^2(X^{i-1}) \le \frac{16i^3}{2^{3n}}$ (non-random bound).
- $\sum_i \mathbf{Ex}(\chi^2(X^{i-1})) \le \frac{18q^4}{2^{3n}}$. So, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{EDM}}(\mathcal{A}) \le \frac{3q^2}{N^{\frac{3}{2}}}$.

Proof Sketch : $\mathsf{EDM}_{\pi,\pi'}(x) = \pi'(\pi(x) \oplus x)$

upper bd $\Pr_{\mathsf{X}}(x_i|x^{i-1}) \leq 1/(2^n - i) \leq \frac{1}{2^n} + \frac{2i}{2^{2n}}$.

lower bd $\Pr_{\mathsf{X}}(x_i|x^{i-1}) \geq \frac{2^n - 4i}{2^n(2^n - i)} \geq \frac{1}{2^n} - \frac{4i}{2^{2n}}$.

$$\left|\Pr_{\mathsf{X}}(x_i|x^{i-1}) - \frac{1}{2^n}\right| \leq \frac{4i}{2^{2n}}.$$

- $\chi^2(X^{i-1}) \leq \frac{16i^3}{2^{3n}}$ (non-random bound).
- $\sum_i \mathbf{Ex}(\chi^2(X^{i-1})) \leq \frac{18q^4}{2^{3n}}$. So, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{EDM}}(\mathcal{A}) \leq \frac{3q^2}{N^{\frac{3}{2}}}$.

Proof Sketch : $\mathsf{EDM}_{\pi,\pi'}(x) = \pi'(\pi(x) \oplus x)$

upper bd $\Pr_{\mathsf{X}}(x_i|x^{i-1}) \leq 1/(2^n - i) \leq \frac{1}{2^n} + \frac{2i}{2^{2n}}$.

lower bd $\Pr_{\mathsf{X}}(x_i|x^{i-1}) \geq \frac{2^n-4i}{2^n(2^n-i)} \geq \frac{1}{2^n} - \frac{4i}{2^{2n}}$.

$$\left|\Pr_{\mathsf{X}}(x_i|x^{i-1}) - \frac{1}{2^n}\right| \leq \frac{4i}{2^{2n}}.$$

- $\chi^2(X^{i-1}) \leq \frac{16i^3}{2^{3n}}$ (non-random bound).
- $\sum_i \mathbf{Ex}(\chi^2(X^{i-1})) \leq \frac{18q^4}{2^{3n}}$. So, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{EDM}}(\mathcal{A}) \leq \frac{3q^2}{N^{\frac{3}{2}}}$.

Proof Sketch : $\mathsf{EDM}_{\pi,\pi'}(x) = \pi'(\pi(x) \oplus x)$

upper bd $\Pr_{\mathsf{X}}(x_i|x^{i-1}) \leq 1/(2^n - i) \leq \frac{1}{2^n} + \frac{2i}{2^{2n}}$.

lower bd $\Pr_{\mathsf{X}}(x_i|x^{i-1}) \geq \frac{2^n - 4i}{2^n(2^n - i)} \geq \frac{1}{2^n} - \frac{4i}{2^{2n}}$.

$$\left| \Pr_{\mathsf{X}}(x_i|x^{i-1}) - \frac{1}{2^n} \right| \leq \frac{4i}{2^{2n}}.$$

- $\chi^2(X^{i-1}) \leq \frac{16i^3}{2^{3n}}$ (non-random bound).
- $\sum_i \mathbf{Ex}(\chi^2(X^{i-1})) \leq \frac{18q^4}{2^{3n}}$. So, $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{EDM}}(\mathcal{A}) \leq \frac{3q^2}{N^{\frac{3}{2}}}$.

Outline of the talk

Construction

1. Let $m \le n$ and trunc_m denote the function which returns the first m bits of $x \in \{0,1\}^n$.
2. We define for every $x \in \{0,1\}^n$,

$$\mathsf{trRP}_m(x) = \mathsf{trunc}_m(\mathsf{RP}_n(x)).$$

   Note that it is a function family, keyed by random permutation, mapping the set of all n bits to the set of all m bits.
3. Let $\mathsf{X}_1, \ldots, \mathsf{X}_q$ denote all outputs of the construction to the adversary then $\mathsf{X}_i = \mathsf{trunc}_m(\mathsf{V}_i)$ for all i.

Proof Sketch : $\mathsf{trRP}_m(x) = \mathsf{trunc}_m(\mathsf{RP}(x))$

- $\Pr_{\mathsf{X}}(x_i|x^{i-1}) = \frac{2^{n-m}-\mathsf{H}}{2^n-i+1}$ where H follows Hypergeomtric distribution (HG).
- $\chi^2(x^{i-1}) = \sum_x \frac{2^m}{(2^n-i+1)^2} \times \left(\mathsf{H} - \frac{i-1}{2^m}\right)^2$
- By using expectation and variance formula of HG and χ^2 method, we have

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{trRP}_m}(\mathcal{A}) \leq \left(\frac{1}{2}\sum_{i=1}^{q}\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})]\right)^{\frac{1}{2}} \leq \frac{q \times 2^{(m-1)/2}}{2^n}.$$

Theorem for trRP_m

Theorem

For any adversary $\mathcal{A}$ making q queries we have

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{trRP}_m}(\mathcal{A}) \leq \frac{q \times 2^{(m-1)/2}}{2^n}.$$

1. When, $m = n$ (no truncation), PRF advantage is $O(q/2^{n/2})$ (again, the presence of square root).
2. When $m = 1$ (returns only one bit), PRF advantage is $O(q/2^n)$.
3. When $m = n/2$ (mid-way : returns half of the bits), PRF advantage is $O(q/2^{3n/4})$.

Outline of the talk

XOR Construction

1. Define $\mathsf{XOR}_\pi : \{0,1\}^{n-1} \to \{0,1\}^n$ to be the construction that takes a permutation $\pi \in \mathsf{Perm}_n$ as a key, and on input $x \in \{0,1\}^{n-1}$ it returns $\pi(x\|0) \oplus \pi(x\|1)$.
2. XOR construction based on a random permutation RP_n returns $\mathsf{X}_1, \ldots, \mathsf{X}_q$ where $\mathsf{X}_1 := \mathsf{V}_1 \oplus \mathsf{V}_2$, $\ldots$, $\mathsf{X}_q := \mathsf{V}_{2q-1} \oplus \mathsf{V}_{2q}$ and $\mathsf{V}_1, \ldots, \mathsf{V}_{2q} \leftarrow_{\text{wor}} \{0,1\}^n$.
3. Mirror theory and H-coefficients proves the PRF security.

Sum of Permutations.

Theorem (DHT-Crypto-17)

Fix an integer $n \geq 8$ and let $N = 2^n$. For any adversary $\mathcal{A}$ that makes $q \leq \frac{N}{32}$ queries we have

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XOR}}(\mathcal{A}) \leq \frac{1.5q + 3\sqrt{q}}{N}.$$

1. $\mathsf{U}'_1, \ldots, \mathsf{U}'_q \leftarrow_{\$} \{0,1\}^n$.
2. Let $\mathbf{P_1}$ and $\mathbf{P_2}$ denote the output distributions of $\mathsf{X} := (\mathsf{X}_1, \ldots, \mathsf{X}_q)$ and $\mathsf{U}' := (\mathsf{U}'_1, \ldots, \mathsf{U}'_q)$ respectively. Thus,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XOR}}(\mathcal{A}) \leq \|\mathbf{P_1} - \mathbf{P_2}\|.$$

Sum of Permutations.

1. $\mathbf{P_0}$ is the probability function for $(\mathsf{U}_1, \ldots, \mathsf{U}_q) \leftarrow_{\text{wr}} [N]^* := \{0,1\}^n \setminus \{0^n\}$.
2. $\|\mathbf{P_0} - \mathbf{P_2}\| \leq q/2^n$.
3. It is sufficient to bound $\|\mathbf{P_0} - \mathbf{P_1}\|$.
4. For every non-zero $x_1, \ldots, x_i$ we clearly have $\mathbf{P}_{\mathbf{0}|x^{i-1}}(x_i) = 1/(N-1)$.

$$\chi^2(x^{i-1}) = \sum_{x \neq 0^n} (N-1)(Y_{i,x} - \frac{1}{N-1})^2. \tag{1}$$

where $Y_{i,x} := \Pr(\mathsf{X}_i = x | \mathsf{X}^{i-1} = x^{i-1})$.

Sum of Permutations.

1. $\mathsf{S} = \{\mathsf{V}_1, \mathsf{V}_2, \ldots, \mathsf{V}_{2i-2}\}$.
2. Let $\mathsf{D}_{i,x}$ be the number of pairs $(u, u \oplus x)$ such that both u and $u \oplus x$ belongs to S.
3. Note that S and $\mathsf{D}_{i,x}$ are both random variables, and in fact functions of the random variables $\mathsf{V}_1, \mathsf{V}_2, \ldots, \mathsf{V}_{2i-2}$.

$$\mathsf{Y}_{i,x} = \frac{N - 4(i-1) + \mathsf{D}_{i,x}}{(N - 2i + 1)(N - 2i)}. \tag{2}$$

Sum of Permutations.

1. $$(\mathsf{Y}_{i,x} - \frac{1}{N-1})^2 \leq \frac{3(\mathsf{D}_{i,x} - 4(i-1)^2/N)^2 + 18}{N^4}.$$

$$\mathbf{Ex}(\chi^2(\mathsf{X}^{i-1})) \leq \sum_{x \neq 0^n} N \cdot \mathbf{Ex}[(\mathsf{Y}_{i,x} - \frac{1}{N-1})^2] \quad (3)$$

$$\leq \sum_{x \neq 0^n} \frac{18}{N^3} + \frac{3}{N^3} \cdot \mathbf{Ex}[(\mathsf{D}_{i,x} - \frac{4(i-1)^2}{N})^2] \quad (4)$$

2. $\mathsf{D}_{i,x}$ as a function of $\mathsf{V}_1, \mathsf{V}_2, \ldots, \mathsf{V}_{2i-2}$, and the expectation is taken over the choices of $\mathsf{V}_1, \mathsf{V}_2, \ldots, \mathsf{V}_{2i-2}$.

$$\mathbf{Ex}[(\mathsf{D}_{i,x} - \frac{4(i-1)^2}{N})^2] \leq \frac{4(i-1)^2}{N} \tag{5}$$

$$\mathbf{Ex}(\chi^2(\mathsf{X}^{i-1})) \leq \frac{18}{N^2} + \frac{12(i-1)^2}{N^3}.$$

Summing up, from χ^2-method

$$\|\mathbf{P_0} - \mathbf{P_1}\| \leq \left(\frac{1}{2}\sum_{i=1}^{q} \mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})]\right)^{\frac{1}{2}}$$
$$\leq \frac{3\sqrt{q} + .5q}{N}. \qquad \square$$

1. Is everything OK?
2. we have

$$\mathbf{P}[\mathsf{X}_i = x | \mathsf{V}_1 = v_1, \ldots, \mathsf{V}_{2i-2} = v_{2i-2}] = \frac{N - 4(i-1) + D_{i,x}}{(N-2i+1)(N-2i)} \quad (6)$$

But,

$$\mathbf{P}[\mathsf{X}_i = x | \mathsf{V}^{2i-2} = v^{2i-2}] = \mathbf{P}[\mathsf{X}_i = x | \mathsf{X}^{i-1} = x^{i-1}] \quad (7)$$

does not hold for every $v_1, \ldots, v_{2i-2}$**.**

1. Is everything OK?
2. we have

$$\mathbf{P}[\mathsf{X}_i = x | \mathsf{V}_1 = v_1, \ldots, \mathsf{V}_{2i-2} = v_{2i-2}] = \frac{N - 4(i-1) + D_{i,x}}{(N - 2i + 1)(N - 2i)} \tag{6}$$

But,

$$\mathbf{P}[\mathsf{X}_i = x | \mathsf{V}^{2i-2} = v^{2i-2}] = \mathbf{P}[\mathsf{X}_i = x | \mathsf{X}^{i-1} = x^{i-1}] \tag{7}$$

does not hold for every $v_1, \ldots, v_{2i-2}$**.**

How to get rid of it?

1. Consider an extended system which leaks more (similar to H technique).
2. Release V_i values in real world. In the ideal world simulate the V_i values keeping compatibility.
3. We aim a more general useful form of Mirror theory.

Summing Up

1. H-Technique is nowadays in popular (in comparison with game playing technique).
2. Sometimes hard to get optimum bound.
3. χ^2 method can be another useful tool for proving security - mainly for close to optimal security.
4. Mirror theory needs attention. It has high potential,
5. We should also study the potentiality of the other metrics.

Thank You for your attention

$$h''_{\alpha+2} = h_\alpha + (-4a+8)\left[h'_\alpha\right] u_1(\textit{ i.e. first blue term }) + [2\delta(\mu_1) + 2\delta(\mu_2)$$

$$+2\delta(\mu_3)+2\delta(\mu_4)+2\delta(\mu_1 \oplus \theta)+2\delta(\mu_2 \oplus \theta)+2\delta(\mu_3 \oplus \theta) + 2\delta(\mu_4 \oplus \theta)]\left[h'_\alpha\right]$$

$$(\textit{ i.e. terms with a value } \lambda_{(i)} \textit{not compatible with } \varphi = 1 \textit{ equation })$$

$$+ [2\delta(\mu_1 \oplus \mu_2) + 2\delta(\mu_1 \oplus \mu_3) + 2\delta(\mu_1 \oplus \mu_4) + 2\delta(\mu_2 \oplus \mu_3) + 2\delta(\mu_2 \oplus \mu_4)$$

$$+2\delta(\mu_3 \oplus \mu_4)]\left[h'_\alpha\right](\textit{ i.e. first green terms })$$

$$+ 6(a-2)(a-4)\left[h''_\alpha\right] u_2(\textit{ i.e. blue term with } \varphi = 2 \textit{ equations})$$

$$- 15 \cdot 2 \cdot 3 \cdot (2\Delta)a\left[h''_\alpha\right] u_3(\textit{“first red term”}, \textit{ i.e. with } \varphi = 2)$$

$$+ 4\Delta u_4\left[h'_\alpha\right](\textit{ i.e. green term: one dependent equation with } \varphi = 2)$$

$$- 8\Delta a u_5\left[h''_\alpha\right](\textit{ i.e. green term one dependent equation with } \varphi = 3)$$

$$- 4(a-2)(a-4)(a-6)u_6\left[h^{(3)}_\alpha\right](\textit{ i.e. blue term with } \varphi = 3)$$

$$+ 256a^2\Delta u_7\left[h^{(3)}_\alpha\right](\textit{ i.e. red term with } \varphi = 3)$$

$$+ (a-2)(a-4)(a-6)(a-8)u_8\left[h^{(4)}_\alpha\right](\textit{ i.e. blue term with } \varphi = 4)$$

$$- 90a^3\Delta u_9\left[h^{(4)}_\alpha\right] u_9(\textit{ i.e. red term with } \varphi = 4)$$

$$+ 12a^2\Delta u_{10}\left[h^{(3)}_\alpha\right](\textit{ i.e. green term: one dependent equation with } \varphi = 4)$$

$$+ 36 \cdot (2\Delta)^2 u_{11}\left[h''_\alpha\right](\textit{ i.e. green term: two dependent equations with } \varphi = 4)$$