Notes on Property-Preserving Encryption

The first type of specialized encryption scheme that can be used in secure outsourced storage we will look at is property-preserving encryption. This is encryption where some desired property of the plaintexts is intentionally leaked by the ciphertexts. The two main examples we will study are deterministic encryption, which preserves the equality property, and order preserving encryption, which preserves order comparison.

1 Background

Symmetric encryption. A symmetric encryption scheme $SE = (K, Enc, Dec)$ with associated plaintext-space $D$ and ciphertext-space $R$ consists of three algorithms. The randomized key generation algorithm $K$ returns a secret key $K$. The (possibly randomized) encryption algorithm $Enc$ takes the secret key $K$, descriptions of plaintext and ciphertext-spaces $D, R$ and a plaintext $m$ to return a ciphertext $c$. The deterministic decryption algorithm $Dec$ takes the secret key $K$, descriptions of plaintext and ciphertext-spaces $D, R$, and a ciphertext $c$ to return a corresponding plaintext $m$ or a special symbol $\bot$ indicating that the ciphertext was invalid.

Note that the above syntax differs from the usual one in that we specify the plaintext and ciphertext-spaces $D, R$ explicitly. We require the usual correctness condition, namely that $Dec(K, D, R, (Enc(K, D, R, m)) = m$ for all $K$ output by $K$ and all $m \in D$. Finally, we say that $SE$ is deterministic if $Enc$ is deterministic.

IND-CPA. It will also be useful to state an equivalent definition of IND-CPA. Let $LR(\cdot, \cdot, b)$ denote the function that on inputs $m_0, m_1$ returns $m_b$. For a symmetric encryption scheme $SE = (K, Enc, Dec)$ and an adversary $A$ and $b \in \{0,1\}$ consider the following experiment:

$\text{Experiment } \text{Exp}_{SE}^{\text{ind-cpa-}b}(A)$

$K \leftarrow K$

$d \leftarrow A^{Enc(K, LR(\cdot, \cdot, b))}$

Return $d$

We require that each query $(m_0, m_1)$ that $A$ makes to its oracle satisfies $|m_0| = |m_1|$. For an adversary $A$, define its ind-cpa advantage against $SE$ as

$$Adv_{SE}^{\text{ind-cpa}}(A) = \Pr[\text{Exp}_{SE}^{\text{ind-cpa-}1}(A) \text{ outputs } 1] - \Pr[\text{Exp}_{SE}^{\text{ind-cpa-}0}(A) \text{ outputs } 1].$$

Pseudorandom functions (PRFs). It will also be useful to state an equivalent definition of PRFs. A family of functions is a map $F : \text{Keys} \times D \rightarrow R$, where for each key $K \in \text{Keys}$ the map $F(K, \cdot) : D \rightarrow R$ is a function. For an adversary $A$, its prf-advantage against $F$, $Adv_F^{\text{prf}}(A)$, is defined as

$$\Pr[K \leftarrow \text{Keys} : A^{F(K, \cdot)} \text{ outputs } 1] - \Pr[f \leftarrow \text{Func}_{D,R} : A^{f(\cdot)} \text{ outputs } 1].$$
where $\text{Func}_{\mathcal{D}, \mathcal{R}}$ denotes the set of all functions from $\mathcal{D}$ to $\mathcal{R}$.

## 2 Deterministic Encryption

Let $\mathcal{SE} = (\mathcal{K}, \mathcal{Enc}, \mathcal{Dec})$ be a symmetric encryption scheme. We say that $\mathcal{SE}$ is deterministic if $\mathcal{Enc}$ is deterministic. Note that such a scheme cannot be IND-CPA secure because it leaks message equality. We give a definition that intuitively guarantees that this is all that is leaked. The idea is that because deterministic encryption leaks plaintext equality, the adversary $A$ in the IND-CPA experiment is restricted to make only distinct queries on either side of its oracle (as otherwise there is a trivial attack). That is, supposing $A$ makes queries $(m_0^b, m_1^b), \ldots, (m_q^b, m_0^b)$, we require that $m_1^b, \ldots, m_q^b$ are all distinct for $b \in \{0, 1\}$.

**IND-DCPA.** For a symmetric encryption scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{Enc}, \mathcal{Dec})$ and an adversary $A$ and $b \in \{0, 1\}$ consider the following experiment:

\[
\text{Experiment } \text{Exp}^{\text{ind-cpa}-b}_{\mathcal{SE}}(A)
\]

- $K \leftarrow \mathcal{K}$
- $d \leftarrow A^{\text{Enc}(K, \mathcal{LR}; \cdot, b)}$
- Return $d$

We require that each query $(m_0, m_1)$ that $A$ makes to its oracle satisfies $|m_0| = |m_1|$. For an adversary $A$, define its ind-cpa advantage against $\mathcal{SE}$ as

\[
\text{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A) = \Pr\left[\text{Exp}_{\mathcal{SE}}^{\text{ind-cpa}-1}(A) \text{ outputs } 1\right] - \Pr\left[\text{Exp}_{\mathcal{SE}}^{\text{ind-cpa}-0}(A) \text{ outputs } 1\right].
\]

We say that an adversary $A$ is equality-respecting if in the above experiment it always makes queries queries $(m_0^b, m_1^b), \ldots, (m_q^b, m_0^b)$ such that $m_1^b, \ldots, m_q^b$ are all distinct for $b \in \{0, 1\}$. We say that $\mathcal{SE}$ is indistinguishable under distinct chosen-plaintext attack (IND-DCPA) if for every equality-respecting adversary $A$, its ind-cpa advantage $\text{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}$ is sufficiently small.

**Construction.** We can construct an IND-DCPA secure deterministic encryption scheme from any IND-CPA secure randomized encryption scheme and a pseudorandom function. Let $\mathcal{SE} = (\mathcal{K}, \mathcal{Enc}, \mathcal{Dec})$ be a symmetric encryption scheme with plaintext space $\mathcal{D}$, and let $\mathcal{Coins}$ be the coin-space for $\mathcal{Enc}$. Let $F$: $\text{Keys} \times \mathcal{D} \rightarrow \mathcal{Coins}$ be a family of functions. Define the deterministic encryption scheme $\mathcal{SE} = (\mathcal{K}', \mathcal{Enc}', \mathcal{Dec})$ where $\mathcal{K}'$ runs $K_e \leftarrow \mathcal{K}$, $K_f \leftarrow \text{Keys}$, and outputs $(K_e, K_f)$, and $\mathcal{Enc}'$ on inputs $(K_e, K_f)$, $m$ runs $cc \leftarrow F(K_f, m)$, $c \leftarrow \mathcal{Enc}(K_e, m; cc)$ and returns $c$.

## 3 Order-Preserving Encryption

For $A, B \subseteq \mathbb{N}$ with $|A| \leq |B|$, a function $f: A \rightarrow B$ is order-preserving (aka. strictly-increasing) if for all $i, j \in A$, $f(i) > f(j)$ iff $i > j$. We say that deterministic encryption scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{Enc}, \mathcal{Dec})$ with plaintext and ciphertext-spaces $[M], [N]$ for some $N \geq M \in \mathbb{N}$ is order-preserving if $\mathcal{Enc}(K, \cdot)$ is an order-preserving function from $[M]$ to $[N]$ for all $K$ output by $\mathcal{K}$. 
IND-OCPA. Noting that any OPE scheme analogously leaks the order relations among the plaintexts, let us first try generalizing the above approach to take this into account. Namely, let us further require the above queries made by A to satisfy $m^j_0 < m^j_1$ iff $m^i_1 < m^i_1$ for all $1 \leq i, j \leq q$. We call such an A an IND-OCPA adversary for indistinguishability under ordered chosen-plaintext attack.

Surprisingly, no order-preserving encryption scheme can be IND-OCPA.

**Theorem 1.** Let $\mathcal{SE} = (K, \mathcal{Enc}, \mathcal{Dec})$ be an order-preserving encryption scheme with plaintext-space $[M]$ and ciphertext-space $[N]$ for $M, N \in \mathbb{N}$ such that $2^{k-1} \leq N < 2^k$ for some $k \in \mathbb{N}$. Then there exists an IND-OCPA adversary $A$ against $\mathcal{SE}$ such that

$$\text{Adv}^{\text{ind-ocpa}}_{\mathcal{SE}}(A) \geq 1 - \frac{2k}{M-1}.$$  

Furthermore, A runs in time $O(\log N)$ and makes 3 oracle queries.

So, $k$ in the theorem should be almost as large as $M$ for A’s advantage to be small.

We introduce the following concept for the proof. For an order-preserving function $f: [M] \to [N]$ call $i \in \{3, \ldots, M-1\}$ a big jump of $f$ if the $f$-distance to the next point is as big as the sum of all the previous, i.e. $f(i+1) - f(i) \geq f(i) - f(1)$. Similarly we call $i \in \{2, \ldots M-2\}$ a big reverse-jump of $f$ if $f(i) - f(i-1) \geq f(M) - f(i)$. The proof uses the following simple combinatorial lemma.

**Lemma 3.1.** Let $f: [M] \to [N]$ be an order-preserving function and suppose that $f$ has $k$ big jumps (respectively big reverse-jumps). Then $N \geq 2^k$.

*Proof.* (of Lemma 3.1) Let $J = \{j_1, \ldots, j_k\}$ be the set of big jumps of $f$. (Our proof trivially adjusts to the case of big reverse jumps, so we do not address it separately.) We prove by induction that for every $1 \leq i \leq M-1$

$$f(j_i) \geq 2^i + f(1).$$

Since $f(N) \geq f(j_k)$, the statement of the lemma follows.

The base case ($i = 1$) holds since $f(j_1) \geq 2 + f(1)$ is true by the definition of a big jump.

Assume $f(j_i) \geq 2^i + f(1)$ is true for $i = n$. We show that it is also true for $i = n + 1$. We claim that

$$f(j_{n+1}) \geq 2f(j_{n+1} - 1) - f(1) \geq 2f(j_n) - f(1) \geq 2 \cdot (2^n + f(1)) - f(1) = 2^{n+1} + f(1).$$

Above, the first inequality is by definition. The second uses that $j_{n+1} - 1 \geq j_n$, which is true because $f$ is order-preserving and the range is $[N]$. The third is by the induction hypothesis. \hfill \Box

We now move on to the proof of the theorem.

**Proof.** (of Theorem 1) Consider the following ind-ocpa adversary $A$ against $\mathcal{SE}$:

**Adversary** $A^{\mathcal{Enc}(K, \mathcal{LR}(...))}$

$m \leftarrow \{1, \ldots, M-1\}$
$c_1 \leftarrow \mathcal{Enc}(K, \mathcal{LR}(1, m, b))$
$c_2 \leftarrow \mathcal{Enc}(K, \mathcal{LR}(m, m+1, b))$
$c_2 \leftarrow \mathcal{Enc}(K, \mathcal{LR}(m+1, M, b))$
Return 1 if $(c_3 - c_2) > (c_2 - c_1)$
Else return 0
First we claim that
\[
\Pr\left[ \text{Exp}^{\text{ind-ocpa-1}}_{\mathcal{SE}}(A) \text{ outputs 1} \right] \geq \frac{(M - 1) - k}{M - 1} = 1 - \frac{k}{M - 1}.
\]

The reason is that \(m\) is picked independently at random and if \(b = 1\) then \(A\) outputs 1 just when \(m + 1\) is not a big reverse-jump of \(\mathcal{E}nc(K, \cdot)\), and since \(N \leq 2^k\) we know that \(\mathcal{E}nc(K, \cdot)\) has at most \(k\) big reverse-jumps by Lemma 3.1. Similarly,
\[
\Pr\left[ \text{Exp}^{\text{ind-ocpa-0}}_{\mathcal{SE}}(A) \text{ outputs 1} \right] \leq \frac{k}{M - 1}
\]
because if \(b = 0\) then \(A\) outputs 1 just when \(m\) is a big jump of \(\mathcal{E}nc(K, \cdot)\), and since \(N \leq 2^k\) we know that \(\mathcal{E}nc(K, \cdot)\) has at most \(k\) big jumps by Lemma 3.1. Subtracting yields the theorem. Note that \(A\) only needs to pick a random element of \([M]\) and do basic operations on elements of \([N]\), which is \(O(\log N)\) as claimed.

As a result, we use a definition of security for OPE similar to that of PRFs.

**POPF.** Fix an order-preserving encryption scheme \(\mathcal{SE} = (\mathcal{K}, \mathcal{E}nc, \mathcal{D}ec)\) with plaintext-space \(\mathcal{D}\) and ciphertext-space \(\mathcal{R}\), \(|\mathcal{D}| \leq |\mathcal{R}|\). For an adversary \(A\) against \(\mathcal{SE}\), define its popf-advantage (or pseudorandom order-preserving function advantage), \(\text{Adv}^{\text{popf-cca}}_{\mathcal{SE}}(A)\), against \(\mathcal{SE}\) as
\[
\Pr\left[ K \leftarrow \mathcal{K} : A^{\mathcal{E}nc(K, \cdot), \mathcal{D}ec(K, \cdot)} \text{ outputs 1} \right] - \Pr\left[ g \leftarrow \mathcal{OPF}_{\mathcal{D}, \mathcal{R}} : A^{g(\cdot)} \text{ outputs 1} \right].
\]
where \(\mathcal{OPF}_{\mathcal{D}, \mathcal{R}}\) denotes the set of all order-preserving functions from \(\mathcal{D}\) to \(\mathcal{R}\).

**Negative hypergeometric distribution.** We can construct a POPF-secure OPE scheme based on sampling the hypergeometric distribution. Consider the following balls-and-bins model. Assume we have \(N\) balls in a bin out of which \(M\) balls are black and \(N - M\) balls are white. At each step we draw a ball at random, without replacement. with \(M\) black and \(N - M\) white balls in the bin, consider the random variable \(Y\) describing the total number of balls in our sample after we pick the \(x\)-th black ball. This random variable follows the negative hypergeometric (NHG) distribution. Formally,
\[
P_{\text{NHGD}}(y; N, M, x) = \frac{(y-1) \cdot (N-y) \cdot (M-x)}{(N) \cdot (M-x)\cdot (M-1)}.\]

**Construction.** Let \(\text{NHGD}\) be a sampling algorithm for the NHGD with coins-space \(\text{Coins}\). Let \(F: \text{Keys} \times \{0, 1\}^* \rightarrow \text{Coins}\) be a family of functions. Our associated order-preserving encryption scheme \(\mathcal{OPE} = (\mathcal{K}, \mathcal{E}nc, \mathcal{D}ec)\) is defined as follows. The plaintext and ciphertext-spaces are sets of consecutive integers \(\mathcal{D}, \mathcal{R}\), respectively.
\[ \mathcal{E}_{ncK}(D, R, m) \]

\begin{align*}
M &\leftarrow |D| ; N \leftarrow |R| \\
d &\leftarrow \min(D) - 1 ; r \leftarrow \min(R) - 1 \\
x &\leftarrow d + \lceil M/2 \rceil \\
cc &\leftarrow F(K, (D, R, x)) \\
y &\leftarrow \text{NHGD}(R, D, x; cc) \\
\text{If } m = x &\text{ then} \\
\text{Return } y \\
\text{If } m < x &\text{ then} \\
D &\leftarrow \{d + 1, \ldots, x - 1\} \\
R &\leftarrow \{r + 1, \ldots, y - 1\} \\
\text{Else} \\
D &\leftarrow \{x + 1, \ldots, d + M\} \\
R &\leftarrow \{y + 1, \ldots, r + N\} \\
\text{Return } \mathcal{E}_{ncK}(D, R, m) \\
\mathcal{D}_{ecK}(D, R, c) \\
\text{If } |D| = 0 &\text{ then return } \perp \\
M &\leftarrow |D| ; N \leftarrow |R| \\
d &\leftarrow \min(D) - 1 ; r \leftarrow \min(R) - 1 \\
x &\leftarrow d + \lceil M/2 \rceil \\
cc &\leftarrow F(K, (D, R, x)) \\
y &\leftarrow \text{NHGD}(R, D, x; cc) \\
\text{If } c = y &\text{ then} \\
\text{Return } x \\
\text{If } c < y &\text{ then} \\
D &\leftarrow \{d + 1, \ldots, x - 1\} \\
R &\leftarrow \{r + 1, \ldots, y - 1\} \\
\text{Else} \\
D &\leftarrow \{x + 1, \ldots, d + M\} \\
R &\leftarrow \{y + 1, \ldots, r + N\} \\
\text{Return } \mathcal{D}_{ecK}(D, R, c)
\end{align*}

**Correctness.** To show correctness, assume we replace invocations of \( F \) with a lookup table that stores truly random coins. Then we have the following.

**Theorem 2.** Suppose invocations of \( F \) are replaced as above. Then for any (even computationally unbounded) algorithm \( A \) we have

\[ \Pr \left[ A^{g(\cdot)} \text{ outputs } 1 \right] = \Pr \left[ A^{\mathcal{E}_{nc}(D, R, \cdot)} \text{ outputs } 1 \right], \]

where \( g \) denotes an order-preserving function picked at random from \( \text{OPF}_{D, R} \).

**Proof.** Let \( M = |D|, N = |R|, d = \min(D) - 1, \) and \( r = \min(R) - 1 \). We will say that two functions \( g, h : D \to R \) are equivalent if \( g(m) = h(m) \) for all \( m \in D \). (Note that if \( D = \emptyset \), any two functions \( g, h : D \to R \) are vacuously equivalent.) Let \( f \) be any function in \( \text{OPF}_{D, R} \). To prove the theorem, it is enough to show that the function defined by \( \mathcal{E}_{nc}(D, R, \cdot) \) is equivalent to \( f \) with probability \( 1/|\text{OPF}_{D, R}| \). We prove this using strong induction on \( M \) and \( N \).

Consider the base case where \( M = 1 \), i.e., \( D = \{m\} \) for some \( m \), and \( N \geq M \). When it is first called, \( \mathcal{E}_{nc}(D, R, m) \) will determine random coins \( cc \), whereupon future calls are consistent. Note that by definition, \( \text{NHGD}(D, R, m; cc) \) returns \( f(m) \) with probability

\[ P_{\text{NHGD}}(f(m) - r; |R|, 1, 1) = \binom{f(m) - r - 1}{0} \cdot \binom{(N-r)-(f(m)-r)}{0} = \frac{1}{N-r} = \frac{1}{|R|}. \]

Thus, the output of \( \mathcal{E}_{nc}(D, R, m) \) will always be \( f(m) \) with probability \( 1/|R| \), implying that \( \mathcal{E}_{nc}(D, R, m) \) is equivalent to \( f(m) \) with probability \( 1/|R| = 1/|\text{OPF}_{D, R}| \).

Now suppose \( M > 1 \), and \( N \geq M \). As an induction hypothesis assume that for all domains \( D' \) of size \( M' \) and ranges \( R' \) of size \( N' \geq M' \), where either \( M' < M \) or \( M' = M \) and \( N' < N \), and for any function \( f' \) in \( \text{OPF}_{D', R'} \), \( \mathcal{E}_{nc}(D', R', \cdot) \) is equivalent to \( f' \) with probability \( 1/|\text{OPF}_{D', R'}| \).

The first time it is called, \( \mathcal{E}_{nc}(D, R, \cdot) \) first computes \( y \leftarrow \text{NHGD}(D, x; cc) \), where \( x = d + \lceil M/2 \rceil \). Henceforth, future calls are consistent. The algorithm follows one of three routes: if \( x = m \), the algorithm terminates and returns \( y \), if \( m < x \) it will return the output of \( \mathcal{E}_{nc}(D_1, R_1, m) \), and if \( m > x \) it will return the output of \( \mathcal{E}_{nc}(D_2, R_2, m) \), where \( D_1 = \{1, \ldots, x-1\} \), \( R_1 = \{1, \ldots, y-1\} \), and \( D_2 = \{x+1, \ldots, d+M\} \), \( R_2 = \{y+1, \ldots, r+N\} \).
By definition, the hypergeometric distribution, and the probability that \( X \) number of black balls chosen after a sample size we draw a ball at random, without replacement. Consider a random variable \( f \) is equivalent to \( f \) restricted to the domain \( D_1 \), and let \( f_2 \) be \( f \) restricted to the domain \( D_2 \). Note then that \( \mathcal{E}nc(D, \mathcal{R}, \cdot) \) is equivalent to \( f \) if and only if all three of the following events occur:

- **E1:** The invocation of \( \text{NHGD}(\mathcal{R}, D, x; cc) \) returns the value \( f(x) \).
- **E2:** \( \mathcal{E}nc(D_1, \mathcal{R}_1, \cdot) \) is equivalent to \( f_1 \).
- **E3:** \( \mathcal{E}nc(D_2, \mathcal{R}_2, \cdot) \) is equivalent to \( f_2 \).

By the law of conditional probability, and since \( E_2 \) and \( E_3 \) are independent,

\[
P(E_1 \cap E_2 \cap E_3) = P(E_1)P(E_2 \cap E_3 \mid E_1) = P(E_1)P(E_2 \mid E_1)P(E_3 \mid E_1).
\]

\( P(E_1) \) is the negative hypergeometric probability that \( \text{NHGD}(\mathcal{R}, D, y - r) \) will return \( f(x) \), which is

\[
P(E_1) = P_{\text{NHGD}}(f(x) - r; N, M, \lceil M/2 \rceil) = \frac{(\binom{f(x)-r-1}{[M/2]-1}) \left( \binom{N-f(x)+r}{M-[M/2]} \right)}{\binom{N}{M}}.
\]

Assume that \( E_1 \) holds, and thus \( f_1 \) is an element of \( \text{OPF}_{D_1, \mathcal{R}_1} \) and \( f_2 \) is an element of \( \text{OPF}_{D_2, \mathcal{R}_2} \). By definition, \( |\mathcal{R}_1|, |\mathcal{R}_2| < |\mathcal{R}| \), and \( |D_1|, |D_2| \leq |D| \). So the induction hypothesis holds for each, and thus \( \mathcal{E}nc(D_1, \mathcal{R}_1, \cdot) \) is equivalent to \( f_1 \) with probability \( 1/|\text{OPF}_{D_1, \mathcal{R}_1}| = 1/(\binom{|\mathcal{R}_1|}{|D_1|}) \), and \( \mathcal{E}nc(D_2, \mathcal{R}_2, \cdot) \) is equivalent to \( f_2 \) with probability \( 1/|\text{OPF}_{D_2, \mathcal{R}_2}| = 1/(\binom{|\mathcal{R}_2|}{|D_2|}) \). Thus, we have that

\[
P(E_2 \mid E_1) = \frac{1}{\binom{f(x)-r-1}{[M/2]-1}} \quad \text{and} \quad P(E_3 \mid E_1) = \frac{1}{\binom{N-f(x)+r}{M-[M/2]}}.
\]

\[
P(E_1 \cap E_2 \cap E_3) = \binom{N}{M} \left( \frac{\binom{f(x)-r-1}{[M/2]-1}}{\binom{N}{M}} \right) \left( \frac{\binom{N-f(x)+r}{M-[M/2]}}{\binom{N}{M}} \right) = \frac{1}{\binom{N}{M}}.
\]

Therefore, \( \mathcal{E}nc(D, \mathcal{R}, \cdot) \) is equivalent to \( f \) with probability \( 1/(\binom{N}{M}) = 1/|\text{OPF}_D, \mathcal{R}| \). Since \( f \) was an arbitrary element of \( \text{OPF}_{D, \mathcal{R}} \), the result follows.

**Hypergeometric distribution.** It turns out that it is only known how to sample efficiently on large domains from the hypergeometric distribution, so we briefly define this and note that the above scheme can be modified accordingly. Consider the following balls-and-bins model. Assume we have \( N \) balls in a bin out of which \( M \) balls are black and \( N - M \) balls are white. At each step we draw a ball at random, without replacement. Consider a random variable \( X \) that describes the number of black balls chosen after a sample size of \( y \) balls are picked. This random variable has a hypergeometric distribution, and the probability that \( X = x \) for the parameters \( N, M, y \) is

\[
P_{\text{HGD}}(x; N, M, y) = \frac{\binom{y}{x} \cdot \binom{N-y}{M-x}}{\binom{N}{M}}.
\]

Intuitively, this equality means we can view constructing a random order-preserving function \( f \) from \([M]\) to \([N]\) as an experiment where we have \( N \) balls, \( M \) of which are black. Choosing balls randomly without replacement, if the \( y \)-th ball we pick is black then the least unmapped point in the domain is mapped to \( y \) under \( f \).
Leakage. The POPF definition does not give a good understanding of what is leaked by a POPF-secure OPE scheme; that is, what is leaked by a random order-preserving function. It can be shown that for uniformly random plaintexts, roughly the upper-half of the plaintext bits are revealed, while the lower-half are hidden.

4 Using Property-Preserving Encryption

Deterministic and order-preserving encryption can be used in secure outsourced database storage to support a large class of SQL queries. This was done in the CryptDB system [ ]. One has to be very careful when using such systems, since by combining publicly available auxiliary information with the leakage, privacy of the client’s data can be compromised [ ].