Privacy Amplification

Edward Eaton

University of Waterloo

April 18, 2016

- Alice and Bob share some bit string $X \in \{0,1\}^N$

- Alice and Bob share some bit string $X \in \{0,1\}^N$
- This string is mostly private, but Eve has some partial information about the string.

- Alice and Bob share some bit string $X \in \{0,1\}^N$
- This string is mostly private, but Eve has some partial information about the string.
- Alice and Bob do not know what Eve knows, but they know exactly how much she knows.

- Alice and Bob share some bit string $X \in \{0,1\}^N$
- This string is mostly private, but Eve has some partial information about the string.
- Alice and Bob do not know what Eve knows, but they know exactly how much she knows.
- Alice and Bob want to generate a new string (of shorter length), via public discussion, that Eve has no information about.

- Alice and Bob share some bit string $X \in \{0,1\}^N$
- This string is mostly private, but Eve has some partial information about the string.
- Alice and Bob do not know what Eve knows, but they know exactly how much she knows.
- Alice and Bob want to generate a new string (of shorter length), via public discussion, that Eve has no information about.

Can they do this?

They Can - An Example

They Can - An Example

- Alice and Bob share the bitstring $b_1 b_2 \in \{0,1\}^2$

They Can - An Example

- Alice and Bob share the bitstring $b_1 b_2 \in \{0,1\}^2$
- They are aware that Eve knows precisely one of these bits.

They Can - An Example

- Alice and Bob share the bitstring $b_1 b_2 \in \{0,1\}^2$
- They are aware that Eve knows precisely one of these bits.
- Alice and Bob take their new string to be $b_1 \oplus b_2$.

They Can - An Example

- Alice and Bob share the bitstring $b_1 b_2 \in \{0,1\}^2$
- They are aware that Eve knows precisely one of these bits.
- Alice and Bob take their new string to be $b_1 \oplus b_2$.
- No matter which bit Eve knows, she does not know the other, so she does not know the result.

They Can - An Example

- Alice and Bob share the bitstring $b_1 b_2 \in \{0,1\}^2$
- They are aware that Eve knows precisely one of these bits.
- Alice and Bob take their new string to be $b_1 \oplus b_2$.
- No matter which bit Eve knows, she does not know the other, so she does not know the result.
- Alice and Bob have generated a new and entirely private bit via public discussion.

They Can - An Example

- Alice and Bob share the bitstring $b_1 b_2 \in \{0,1\}^2$
- They are aware that Eve knows precisely one of these bits.
- Alice and Bob take their new string to be $b_1 \oplus b_2$.
- No matter which bit Eve knows, she does not know the other, so she does not know the result.
- Alice and Bob have generated a new and entirely private bit via public discussion.

This problem was solved in general by Bennet, Brassard, and Roberts in their 1988 paper *Privacy Amplification by Private Discussion*.

Motivation

- Solving this problem is an important step in Quantum Key Distribution.

Motivation

- Solving this problem is an important step in Quantum Key Distribution.
- In Quantum Key Distribution, Alice sends Bob qubits in order to establish a shared secret, random key that can then be used for symmetric key cryptography.

Motivation

- Solving this problem is an important step in Quantum Key Distribution.
- In Quantum Key Distribution, Alice sends Bob qubits in order to establish a shared secret, random key that can then be used for symmetric key cryptography.
- By sending these qubits to Bob, and engaging in a small amount of non-secret discussion that (effectively) does not leak any information, they establish a shared string $X \in \{0,1\}^N$.

Motivation

- Solving this problem is an important step in Quantum Key Distribution.
- In Quantum Key Distribution, Alice sends Bob qubits in order to establish a shared secret, random key that can then be used for symmetric key cryptography.
- By sending these qubits to Bob, and engaging in a small amount of non-secret discussion that (effectively) does not leak any information, they establish a shared string $X \in \{0,1\}^N$.
- Eve may listen in on the generation of X, so Alice and Bob want to 'remove' any infortmation she may have.

- The *No Cloning Theorem* in Quantum Information Processing states (roughly) that you cannot copy a qubit with high accuracy.

- The *No Cloning Theorem* in Quantum Information Processing states (roughly) that you cannot copy a qubit with high accuracy.
- Implication of this: Extracting information from a qubit generally destroys some information.

- The *No Cloning Theorem* in Quantum Information Processing states (roughly) that you cannot copy a qubit with high accuracy.
- Implication of this: Extracting information from a qubit generally destroys some information.
- If Eve wants to extract information out of the qubits Alice sends to Bob, she alters the qubits Bob receives with high probability, introducing errors.

- The *No Cloning Theorem* in Quantum Information Processing states (roughly) that you cannot copy a qubit with high accuracy.
- Implication of this: Extracting information from a qubit generally destroys some information.
- If Eve wants to extract information out of the qubits Alice sends to Bob, she alters the qubits Bob receives with high probability, introducing errors.
- By examining the error rate, Alice and Bob can obtain a good upperbound on the information Eve has.

Strongly Universal Hash Functions

Definition

Let H be a set of Hash functions from $\{0,1\}^N$ to $\{0,1\}^R$. We say that H is *Strongly Universal*$_2$ if, given any pair of distinct elements $a_1, a_2 \in \{0,1\}^N$, and any pair $b_1, b_2 \in \{0,1\}^N$, we have that exactly $|H|/2^{2R}$ functions in H take a_1 to b_1 and a_2 to b_2.

Strongly Universal Hash Functions

Definition

Let H be a set of Hash functions from $\{0,1\}^N$ to $\{0,1\}^R$. We say that H is *Strongly Universal*$_2$ if, given any pair of distinct elements $a_1, a_2 \in \{0,1\}^N$, and any pair $b_1, b_2 \in \{0,1\}^N$, we have that exactly $|H|/2^{2R}$ functions in H take a_1 to b_1 and a_2 to b_2.

- Example: The set of all functions from $\{0,1\}^N$ to $\{0,1\}^R$.

Strongly Universal Hash Functions

Definition

Let H be a set of Hash functions from $\{0,1\}^N$ to $\{0,1\}^R$. We say that H is *Strongly Universal*$_2$ if, given any pair of distinct elements $a_1, a_2 \in \{0,1\}^N$, and any pair $b_1, b_2 \in \{0,1\}^N$, we have that exactly $|H|/2^{2R}$ functions in H take a_1 to b_1 and a_2 to b_2.

- Example: The set of all functions from $\{0,1\}^N$ to $\{0,1\}^R$.
- Fact: Strongly Universal$_2$ hash functions can be efficiently constructed, sampled, and computed.

- Alice and Bob establish a shared, uniform random $x \in \{0,1\}^N$

- Alice and Bob establish a shared, uniform random $x \in \{0,1\}^N$
- Via public discussion, they select a uniformly random function g from a set H of strongly universal$_2$ hash functions.

- Alice and Bob establish a shared, uniform random $x \in \{0,1\}^N$
- Via public discussion, they select a uniformly random function g from a set H of strongly universal$_2$ hash functions.
- They compute $g(x)$ as their shared key.

- Alice and Bob share a bit string $X \in \{0,1\}^N$.

- Alice and Bob share a bit string $X \in \{0,1\}^N$.
- Eve can choose any function $e : \{0,1\}^N \rightarrow \{0,1\}^K$ and obtain $e(X) \in \{0,1\}^K$.

- Alice and Bob share a bit string $X \in \{0,1\}^N$.
- Eve can choose any function $e : \{0,1\}^N \rightarrow \{0,1\}^K$ and obtain $e(X) \in \{0,1\}^K$.
- Alice and Bob do not know e, but they do know K.

- For $z \in \{0,1\}^R$, $x \in \{0,1\}^N$, $g \in H$, we define

$$\Delta_z^{x,g} = \begin{cases} 1 & \text{if } g(x) = z \\ 0 & \text{otherwise} \end{cases}$$

- For $z \in \{0,1\}^R$, $x \in \{0,1\}^N$, $g \in H$, we define

$$\Delta_z^{x,g} = \begin{cases} 1 & \text{if } g(x) = z \\ 0 & \text{otherwise} \end{cases}$$

- As well, for $A \subseteq \{0,1\}^N$, define

$$\Delta_z^{A,g} = \sum_{x \in A} \Delta_z^{x,g} = \#\{x \in A : g(x) = z\}$$

- For $z \in \{0,1\}^R$, $x \in \{0,1\}^N$, $g \in H$, we define

$$\Delta_z^{x,g} = \begin{cases} 1 & \text{if } g(x) = z \\ 0 & \text{otherwise} \end{cases}$$

- As well, for $A \subseteq \{0,1\}^N$, define

$$\Delta_z^{A,g} = \sum_{x \in A} \Delta_z^{x,g} = \#\{x \in A : g(x) = z\}$$

- And for $F \subseteq H$, define

$$\Delta_z^{x,F} = \sum_{g \in F} \Delta_z^{x,g} = \#\{g \in F : g(x) = z\}$$

Using our new notation, and the definition of strongly universal$_2$, for any $x \in \{0,1\}^N$, choose an arbitrary $x' \in \{0,1\}^N$ with $x' \neq x$.

Using our new notation, and the definition of strongly universal$_2$, for any $x \in \{0,1\}^N$, choose an arbitrary $x' \in \{0,1\}^N$ with $x' \neq x$.

$$\begin{aligned}
\Delta_z^{x,H} &= \#\{g \in H : g(x) = z\} \\
&= \sum_{z' \in \{0,1\}^R} \#\{g \in H : g(x) = z \text{ and } g(x') = z'\} \\
&= \sum_{z' \in \{0,1\}^R} \#H/2^{2R} \\
&= \#H/2^R
\end{aligned}$$

$$
\begin{aligned}
&\sum_{g \in H} \left(\Delta_z^{E,g} \right)^2 \\
=&\sum_{g \in H} \left(\sum_{x \in E} \Delta_z^{x,g} \right)^2 \\
=&\sum_{g \in H} \sum_{x \in E} \sum_{x' \in E} \Delta_z^{x,g} \Delta_z^{x',g} \\
=&\sum_{x \in E} \sum_{x' \in E} \#\{g \in H : g(x) = z \text{ and } g(x') = z\} \\
=&\sum_{x \in E} \#\{g \in H : g(x) = z\} + \sum_{x \neq x'} \#\{g \in H : g(x) = g(x') = z\} \\
=&\#E \#H / 2^R + \#E(\#E - 1)\#H / 2^{2R} \\
=&\#E \#H / 2^R \left(1 + \frac{\#E - 1}{2^R} \right)
\end{aligned}
$$

- Note that we start with a uniformly random element of $\{0,1\}^N$

- Note that we start with a uniformly random element of $\{0,1\}^N$
- When Eve has $e(x)$, we can consider the set

$$E := \{y \in \{0,1\}^N : e(y) = e(x)\}$$

as the set of equally likely candidates for x from Eve's perspective.

- Note that we start with a uniformly random element of $\{0,1\}^N$
- When Eve has $e(x)$, we can consider the set

$$E := \{y \in \{0,1\}^N : e(y) = e(x)\}$$

  as the set of equally likely candidates for x from Eve's perspective.
- Let X be a uniformly random element of E.
- Let G be a uniformly random function in H.
- Let Z be an r.v. over $\{0,1\}^R$ such that if $X = x$ and $G = g$ then $Z = g(x)$.

We want to consider $I(G; Z)$, the mutual information of Z (which we want Eve to not have) and G (which Eve does have).

We want to consider $I(G;Z)$, the mutual information of Z (which we want Eve to not have) and G (which Eve does have).
Note that

$$Pr[Z = z|G = g] = \Delta_z^{E,g}/\#E$$

We want to consider $I(G;Z)$, the mutual information of Z (which we want Eve to not have) and G (which Eve does have).
Note that

$$Pr[Z = z|G = g] = \Delta_z^{E,g}/\#E$$

$$\begin{aligned} Pr[Z = z, G = g] &= Pr[G = g]Pr[Z = z|G = g] \\ &= \Delta_z^{E,g}/\#E\#H \end{aligned}$$

$$
\begin{aligned}
Pr[Z = z] &= \sum_{g \in H} Pr[Z = z, G = g] \\
&= \frac{1}{\#E\#H} \sum_{g \in H} \Delta_z^{E,g} \\
&= \frac{1}{\#E\#H} \sum_{e \in E} \Delta_z^{e,H} \\
&= \frac{1}{\#E\#H} \#E \frac{\#H}{2^R} = 2^{-R}
\end{aligned}
$$

Using an (equivalent) definition of Mutual Information

$$I(Z;G) = \sum_{z \in \{0,1\}^R} \sum_{g \in H} Pr[Z = z, G = g] \log \frac{Pr[Z = z | G = g]}{Pr[Z = z]}$$

$$= \sum_{z} \sum_{g} \frac{\Delta_z^{E,g}}{\#E\#H} \log \frac{\Delta_z^{E,g} 2^R}{\#E}$$

$$= 2^{-R} \sum_{z} \sum_{g} \Delta_z^{E,g} \frac{2^R}{\#E\#H} \log \frac{\Delta_z^{E,g} 2^R}{\#E}$$

Using an (equivalent) definition of Mutual Information

$$I(Z;G) = \sum_{z \in \{0,1\}^R} \sum_{g \in H} Pr[Z = z, G = g] \log \frac{Pr[Z = z | G = g]}{Pr[Z = z]}$$

$$= \sum_z \sum_g \frac{\Delta_z^{E,g}}{\#E\#H} \log \frac{\Delta_z^{E,g} 2^R}{\#E}$$

$$= 2^{-R} \sum_z \sum_g \Delta_z^{E,g} \frac{2^R}{\#E\#H} \log \frac{\Delta_z^{E,g} 2^R}{\#E}$$

Note that

$$\sum_g \Delta_z^{E,g} 2^R / \#E\#H = 1$$

and so we can use Jensen's Inequality

$$
\begin{aligned}
I(Z;G) \leq & 2^{-R} \sum_z \log \left[\sum_g \Delta_z^{E,g} \frac{2^R}{\#E\#H} \frac{\Delta_z^{E,g} 2^R}{\#E} \right] \\
= & 2^{-R} \sum_z \log \left[\frac{2^{2R}}{\#E^2\#H} \sum_g (\Delta_z^{E,g})^2 \right] \\
= & 2^{-R} \sum_z \log \left[\frac{2^R}{\#E} \left(1 + \frac{\#E - 1}{2^R} \right) \right] \\
= & \log \left[\frac{2^R + \#E - 1}{\#E} \right] \\
< & \log \left[1 + \frac{2^R}{\#E} \right]
\end{aligned}
$$

Let $e : \{0,1\}^N \rightarrow \{0,1\}^K$ be any function.
Let $S < N - K$ be a security parameter.
Let $R = N - K - S$

Let $e : \{0,1\}^N \rightarrow \{0,1\}^K$ be any function.
Let $S < N - K$ be a security parameter.
Let $R = N - K - S$

Theorem

If $g : \{0,1\}^N \rightarrow \{0,1\}^R$ is chosen randomly, the expected amount of information on $g(x)$ given by g, e, and $e(x)$ is less than $\log(1 + 2^{-S})$ bits.

Let $E_x = \{y \in \{0,1\}^N : e(y) = e(x)\}$

Let $E_x = \{y \in \{0,1\}^N : e(y) = e(x)\}$
Each $x \in \{0,1\}^N$ is equally likely. So we have that the knowledge of $g(x)$ given by g, e, and $e(x)$ is (in expectation) less than

Let $E_x = \{y \in \{0,1\}^N : e(y) = e(x)\}$
Each $x \in \{0,1\}^N$ is equally likely. So we have that the knowledge of $g(x)$ given by g, e, and $e(x)$ is (in expectation) less than

$$\begin{aligned}
&\sum_{x \in \{0,1\}^N} 2^{-N} \log\left(1 + \frac{2^R}{\#E_x}\right) \\
&\leq \log\left(\sum_x 2^{-N} + 2^{R-N}/\#E_x\right) \\
&= \log\left(1 + 2^{-S}2^{-K}\sum_x \frac{1}{\#E_x}\right) \\
&\leq \log(1 + 2^{-S})
\end{aligned}$$

As $\sum 1/\#E_x \leq 2^K$

- By choosing a sensible security parameter, Eve's information is reduced to an amount arbitrarily close to zero

- By choosing a sensible security parameter, Eve's information is reduced to an amount arbitrarily close to zero
- Alice and Bob can then safely use their newly established secret for symmetric key cryptography

Thank You