Two views on cryptographic reductions

Sven Laur[♠]
swen@math.ut.ee

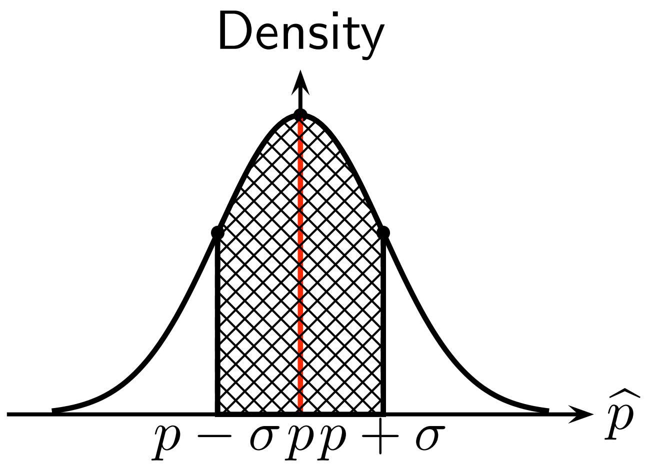
Helsinki University of Technology

♠ The presentation is based on the joint work with
Ahto Buldas, Emilia Käsper and Helger Lipmaa

Estimating the bias of a coin causes collapse

Before measurement

$$\widehat{p} = \frac{1}{n} \sum_{i=1}^{n} X_i$$



With probability 68.3% the difference $|\widehat{p} - p_{\mathrm{true}}| \leq \sigma \leq \frac{1}{2\sqrt{n}}$.

After measurement

$$\Pr\left[\widehat{p} \in (p - \sigma, p + \sigma)\right] = 1$$

or

$$\Pr\left[\widehat{p} \notin (p - \sigma, p + \sigma)\right] = 1$$

The measurement causes collapse classical statistics!

Choosing a hash function cause a collapse

Before measurement

Let $\mathcal{H}$ be a hash function family

$$\mathcal{H} \ni h : \{0,1\}^* \to \{0,1\}^\ell$$

Pick any t-time adversarial code A
The hash family $\mathcal{H}$ is (t, ε)-secure if

$$\underbrace{\Pr\left[\begin{array}{l} h \leftarrow \mathcal{H}, (x_1, x_2) \leftarrow \mathsf{A}(h) : \\ h(x_1) = h(x_2) \wedge x_1 \neq x_2 \end{array}\right]}_{\mathsf{Adv}^{\mathsf{coll}}_{\mathcal{H}}(\mathsf{A})} \leq \varepsilon$$

The guarantee is given for $\mathcal{H}$.

After measurement

SHA-1 is used in standards!

A :

$x_0 =$ `0x010ed...`

$x_1 =$ `0x03ffe...`

return (x_0, x_1)

Breaks SHA-1 in constant time!
Classical cryptography collapses!

Why do we use SHA-1?

SHA-1 algorithms were published by US National Security Agency in 1995.

SHA-1 is belived to be collision resistant

- as SHA-1 as withstand all currently known cryptanalytic attacks
- The best known attack on SHA-1 takes 2^{69} hash operations

SHA-1 and MD-5 were used as it was reasonable to believe

No human can produce a t-time algorithm with success probability more than ε.

Such statements are inherently subjective and can be never proved.

Proper formulation of the security belief

Let $\mathcal{D}_{\mathrm{code}}$ be a distribution of t-time programs.

We say that a fixed hash function $h : \{0,1\}^* \rightarrow \{0,1\}^\ell$ is (t,ε)-collision resistant with respect to the distribution $\mathcal{D}_{\mathrm{code}}$ if

$$\Pr\left[\mathsf{A} \leftarrow \mathcal{D}_{\mathrm{code}}, (x_0, x_1) \leftarrow \mathsf{A}(h) : \ h(x_0) = h(x_1) \wedge x_0 \neq x_1 \ \right] \leq \varepsilon \ .$$

The prior belief what kind of $\mathcal{D}_{\mathrm{code}}$ is accessible to adversaries can change:

- MD5 and SHA-1 were believed to be $(2^{80}, 2^{-80})$-collision resistant (1995).
- MD5 is now totally insecure (2005).
- SHA-1 is only $(2^{69}, 1)$-collision resistant (2005).

How should one prove security?

How to prove that a primitive $\mathfrak{P}_2$ is secure if the primitive $\mathfrak{P}_1$ is secure?

We can prove this only under the assumption that adversaries are rational and our prior code distributions $\mathcal{D}_{\mathrm{code}}(\mathfrak{P}_1)$ and $\mathcal{D}_{\mathrm{code}}(\mathfrak{P}_2)$ are rational.

Distributions $\mathcal{D}_{\mathrm{code}}(\mathfrak{P}_1)$ and $\mathcal{D}_{\mathrm{code}}(\mathfrak{P}_2)$ are related if

- we can give an efficient rule Complile how to transform a successful adversary $\mathsf{A} \leftarrow \mathcal{D}_{\mathrm{code}}(\mathfrak{P}_2)$ to Complile(A) that can efficiently attack $\mathfrak{P}_1$.

Then it is inconsistent to assume that $\mathfrak{P}_2$ is insecure w.r.t. $\mathcal{D}_{\mathrm{code}}(\mathfrak{P}_2)$ and $\mathfrak{P}_1$ is secure w.r.t. $\mathcal{D}_{\mathrm{code}}(\mathfrak{P}_1) \Longrightarrow \mathfrak{P}_2$ must be secure w.r.t. $\mathcal{D}_{\mathrm{code}}(\mathfrak{P}_2)$.

How does it effect cryptographic reductions?

Security bounds obtained by true black-box reductions remain intact.

- Fundamental results in cryptography hold in both formalisations

Parametric black-box reductions degrade slightly.

- E.g. all reductions where something is repeated $n(\mathsf{A})$ times.

Most white-box reductions fail, as they have inefficient Complile rule.

- Many reductions can be done only with white-box methodologies.