



NTNU

Norwegian University of
Science and Technology

NESTED PROGRAM LOGIC FOR EASYCRYPT

Oskar Goldhahn

October 30, 2025

Contents

Formal Verification

Program Logics in EasyCrypt

Correctness and Nesting

Formal Verification

What

Checking/generating proofs using computers

Why

Humans make mistakes, both in implementation and security proofs

Formal Verification

What

Checking/generating proofs using computers

Why

Humans make mistakes, both in implementation and security proofs

EasyCrypt is a proof assistant for writing machine-checkable security proofs.

Hoare Logic

$\{P\}C\{Q\}$, where C is a program and P and Q are predicates over program state

Semantics of Hoare Triples

For every initial state such that P holds then when running C if we terminate Q holds for the final state.

Hoare Logic

$\{P\}C\{Q\}$, where C is a program and P and Q are predicates over program state

Semantics of Hoare Triples

For every initial state such that P holds then when running C if we terminate Q holds for the final state.

$$\begin{array}{c} \frac{}{\{P\}\text{skip}\{P\}} \quad \frac{}{\{P[e/x]\}x := e\{P\}} \quad \frac{\{P\}F\{Q\} \quad \{Q\}S\{R\}}{\{P\}F; S\{R\}} \\ \frac{\{P \wedge B\}F\{Q\} \quad \{P \wedge \neg B\}S\{Q\}}{\{P\}\text{if } B \text{ then } F \text{ else } S\{Q\}} \quad \frac{P' \Rightarrow P \quad \{P\}C\{Q\} \quad Q \Rightarrow Q'}{\{P'\}C\{Q'\}} \\ \frac{\{P \wedge B\}C\{P\}}{\{P\}\text{while } B \text{ do } C\{P \wedge \neg B\}} \quad \frac{}{\{\text{true}\}\text{abort}\{\text{false}\}} \end{array}$$

Probabilistic Hoare Logic

$$\{P\}C\{Q\} \geq p$$

For all initial states such that P holds, when running C we terminate with a final state satisfying Q with probability at least p .

Probabilistic Hoare Logic

$$\{P\}C\{Q\} \geq p$$

For all initial states such that P holds, when running C we terminate with a final state satisfying Q with probability at least p .

$$\frac{}{\{T\}C\{\perp\} \geq 0} \quad \frac{\{P\}C\{Q\} \geq p \quad \{P\}C\{R\} \geq q}{\{P\}C\{Q \wedge R\} \geq p + q - 1}$$

Correctness for encrypting twice

Correct^S(m)

$sk, pk \leftarrow \$ \mathcal{S}.\mathcal{KG}$

$c \leftarrow \$ \mathcal{S}.\text{Enc}(pk, m)$

$m' \leftarrow \$ \mathcal{S}.\text{Dec}(sk, c)$

$r \leftarrow (m' = m)$

NestedCorrect^{S₁,S₂}(m)

$sk_1, pk_1 \leftarrow \$ \mathcal{S}_1.\mathcal{KG}$

$sk_2, pk_2 \leftarrow \$ \mathcal{S}_2.\mathcal{KG}$

$c_1 \leftarrow \$ \mathcal{S}_1.\text{Enc}(pk_1, m)$

$c_2 \leftarrow \$ \mathcal{S}_2.\text{Enc}(pk_2, c_1)$

$c'_1 \leftarrow \$ \mathcal{S}_2.\text{Dec}(sk_2, c_2)$

$m' \leftarrow \$ \mathcal{S}_1.\text{Dec}(sk_1, c'_1)$

$r \leftarrow (m' = m)$

Correctness for encrypting twice

$$\frac{\text{Correct}^{\mathcal{S}}(m)}{\text{---}}$$
$$sk, pk \leftarrow \$ \mathcal{S}.\mathcal{KG}$$
$$c \leftarrow \$ \mathcal{S}.\text{Enc}(pk, m)$$
$$m' \leftarrow \$ \mathcal{S}.\text{Dec}(sk, c)$$
$$r \leftarrow (m' = m)$$
$$\frac{\text{NestedCorrect}^{\mathcal{S}_1, \mathcal{S}_2}(m)}{\text{---}}$$
$$sk_1, pk_1 \leftarrow \$ \mathcal{S}_1.\mathcal{KG}$$
$$sk_2, pk_2 \leftarrow \$ \mathcal{S}_2.\mathcal{KG}$$
$$c_1 \leftarrow \$ \mathcal{S}_1.\text{Enc}(pk_1, m)$$
$$c_2 \leftarrow \$ \mathcal{S}_2.\text{Enc}(pk_2, c_1)$$
$$c'_1 \leftarrow \$ \mathcal{S}_2.\text{Dec}(sk_2, c_2)$$
$$m' \leftarrow \$ \mathcal{S}_1.\text{Dec}(sk_1, c'_1)$$
$$r \leftarrow (m' = m)$$

$$\forall x, \{m = x\} \text{Correct}^{\mathcal{S}_1} \{r = \top\} \wedge (\forall x', \{m = x'\} \text{Correct}^{\mathcal{S}} \{r = \top\}) \Rightarrow \\ \{m = x\} \text{NestedCorrect}^{\mathcal{S}_1, \mathcal{S}_2}(m) \{r = \top\}$$

Correctness with Nesting

$$\begin{aligned} & \{\top\} \text{sk}, \text{pk}, \leftarrow \$ \mathcal{S}.\mathcal{KG}\{ \\ & \quad \forall \text{sk}', \forall \text{pk}', \forall m', \text{sk} = \text{sk}' \wedge \text{pk} = \text{pk}' \Rightarrow \\ & \quad \{\text{pk} = \text{pk}' \wedge m = m'\} \mathcal{S}.\text{Enc}\{ \\ & \quad \quad \forall c', c = c' \Rightarrow \\ & \quad \quad \{c = c'\} \mathcal{S}.\text{Dec}\{m = m'\} \\ & \quad \} \\ & \} \end{aligned}$$

Correctness with Nesting

$$\begin{aligned} & \{\top\} \text{sk}, \text{pk}, \leftarrow \$ \mathcal{S}.\mathcal{KG}\{ \\ & \quad \forall \text{sk}', \forall \text{pk}', \forall m', \text{sk} = \text{sk}' \wedge \text{pk} = \text{pk}' \Rightarrow \\ & \quad \{\text{pk} = \text{pk}' \wedge m = m'\} \mathcal{S}.\text{Enc}\{ \\ & \quad \quad \forall c', c = c' \Rightarrow \\ & \quad \quad \{c = c'\} \mathcal{S}.\text{Dec}\{m = m'\} \\ & \quad \} \\ & \} \end{aligned}$$

$$\frac{\{P\}C_1; C_2\{R\}}{\{P\}C_1\{\exists Q, Q \wedge \{Q\}C_2\{R\}\}}$$

Correctness with Nesting

$$\begin{aligned} & \{\top\} \text{sk}, \text{pk}, \leftarrow \$ \mathcal{S}.\mathcal{KG}\{ \\ & \quad \forall \text{sk}', \forall \text{pk}', \forall m', \text{sk} = \text{sk}' \wedge \text{pk} = \text{pk}' \Rightarrow \\ & \quad \{\text{pk} = \text{pk}' \wedge m = m'\} \mathcal{S}.\text{Enc}\{ \\ & \quad \quad \forall c', c = c' \Rightarrow \\ & \quad \quad \{c = c'\} \mathcal{S}.\text{Dec}\{m = m'\} \\ & \quad \} \\ & \} \end{aligned}$$

$$\frac{\{P\}C_1; C_2\{R\}}{\{P\}C_1\{\exists Q, Q \wedge \{Q\}C_2\{R\}\}}$$

$$\frac{\forall x, \{P\}C\{R(x)\}}{\{P\}C\{\forall x, R(x)\}}$$

Partial Correctness

$$\begin{aligned} & \{\top\} \text{sk}, \text{pk}, \leftarrow \$ \mathcal{S}.\mathcal{KG}\{ \\ & \quad \forall \text{sk}', \forall \text{pk}', \forall m', \text{sk} = \text{sk}' \wedge \text{pk} = \text{pk}' \Rightarrow \\ & \quad \{\text{pk} = \text{pk}' \wedge m = m'\} \mathcal{S}.\text{Enc}\{ \\ & \quad \quad \forall c', c = c' \Rightarrow \\ & \quad \quad \{c = c'\} \mathcal{S}.\text{Dec}\{m = m'\} \geq p_3 \\ & \quad \} \geq p_2 \\ & \} \geq p_1 \end{aligned}$$

Questions?

- [1] Gilles Barthe. *An introduction to relational program verification*. URL: https://software.imdea.org/~gbarthe/_intrelover.pdf.