Privacy Enhancing Technologies (BSc)

Exercise II: Proofs and Theoretical Deepening

Paul Gerhart

November 18, 2024

Overview

KW	Type	Lectures
42	**Lecture**	Internet and Privacy in the Web
43	**Lecture**	Fingerprinting & Censorship
44	**Exercise**	Introduction to Rust & Challenge Start
45	**Lecture**	Cryptographic Preliminaries
46	**Lecture**	Public Key Cryptography and Security Reductions
47	**Exercise**	**Proofs and Theoretical Deepening**
48	**Lecture**	TLS
49	**Exam**	**Midterm Exam**
50	**Exercise**	Challenge Hands-On
51	**Lecture**	Messaging I
3	**Lecture**	Messaging II (Forward Security, Post Compromise Security)
4	**Lecture**	Onion
5	**Lecture**	Q & A
6	**Exam**	**Final Exam**
9	**Exam**	**Reexam** (Both for Midterm and Final)

This Lecture's Agenda

- Construction of El Gamal encryption
- Proof of El Gamal encryption
- Deepening on reduction proofs

El Gamal Encryption

Notation

If we talk about group elements $g^x \in \mathbb{G}$, where the generator g is known, we use the notation $g^x = [x]$.
By $x \leftarrow\!\!\$\ X$, we denote the uniform sampling of x from the set X, and λ represents the security parameter. By $y \leftarrow \mathsf{A}(x; r)$ we denote a probabilistic polynomial time (PPT) algorithm A that on input x and randomness r, outputs y. When A is a deterministic polynomial time (DPT) algorithm, we use the notation $x := \mathsf{A}(y)$. We call a function $\mathsf{negl}(\lambda) : \mathbb{N} \to \mathbb{R}$ negligible in λ if for every $k \in \mathbb{N}$, there exists $\lambda_0 \in \mathbb{N}$ s.t. for every $\lambda \geq \lambda_0$ it holds that $|\mathsf{negl}(\lambda)| \leq \lambda^{-k}$.

El Gamal Encryption Scheme

Construction

We define the El Gamal encryption scheme as follows:

$\mathsf{KGen}(\lambda)$	$\mathsf{Enc}(\mathsf{pk}, m)$	$\mathsf{Dec}(\mathsf{sk}, c)$
$(\mathbb{G}, q, g) \leftarrow \mathsf{Pgen}(1^\lambda)$	$(m \in \mathbb{G})$	$\langle c_1, c_2 \rangle := c$
$x \xleftarrow{\$} \mathbb{Z}_q$	$y \xleftarrow{\$} \mathbb{Z}_q$	$m := \frac{c_2}{c_1^x}$
$h := [x]$	$c_1 := [y]$	**return** m
$\mathsf{sk} := \langle \mathbb{G}, q, g, x \rangle$	$c_2 := \mathsf{pk}^y \cdot m$	
$\mathsf{pk} := \langle \mathbb{G}, q, g, h \rangle$	**return** $\langle c_1, c_2 \rangle$	
return $(\mathsf{sk}, \mathsf{pk})$		

Security of El Gamal Encryption

Theorem

If the DDH problem is hard relative to $\mathbb{G}$, then the El Gamal encryption scheme is CPA secure.

Lemma

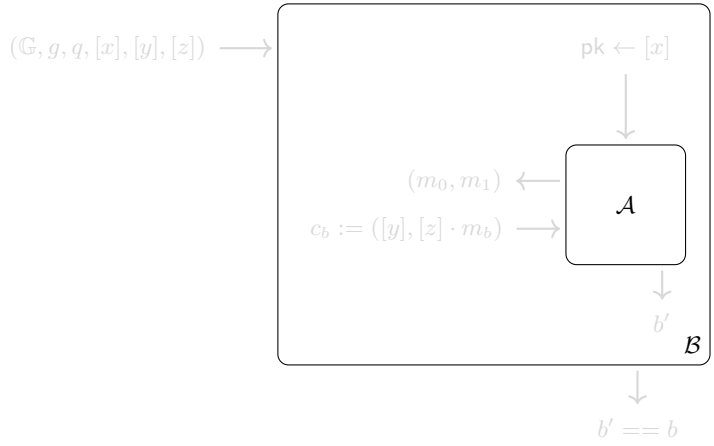
Let $\mathbb{G}$ be a finite group and $m \in \mathbb{G}$ be arbitrary. Then choosing uniform $k \leftarrow \mathbb{G}$ and setting $k' := k \cdot m$ gives the same distribution for k' as choosing uniform $k' \leftarrow \mathbb{G}$. Put differently, for any $g'' \in \mathbb{G}$ we have

$$\Pr[k \cdot m = g''] = \frac{1}{|\mathbb{G}|},$$

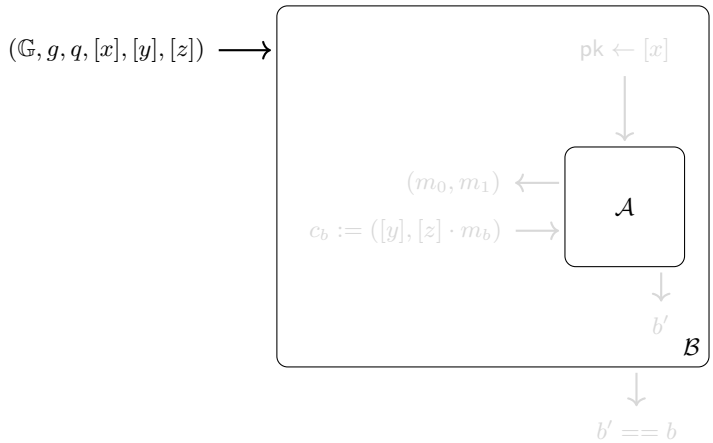
where the probability is taken over a uniform choice of k.

Proof

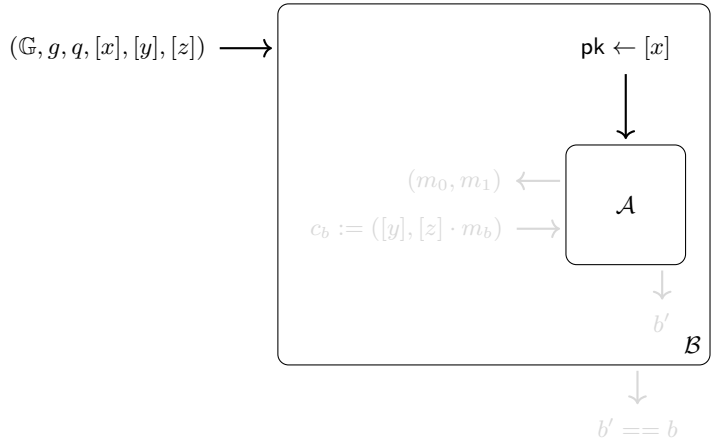
Proof of El Gamal



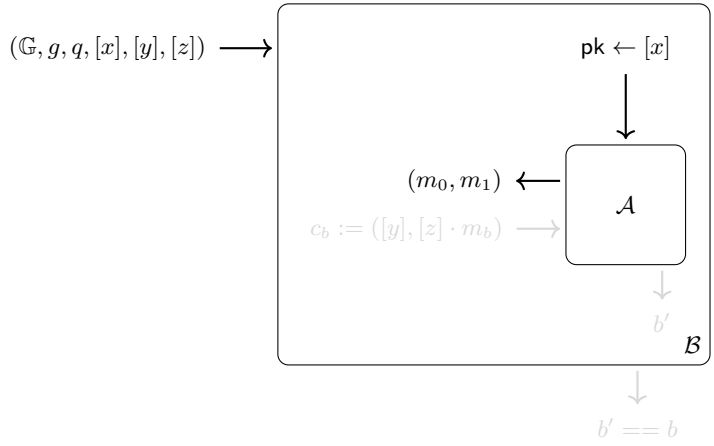
Proof of El Gamal



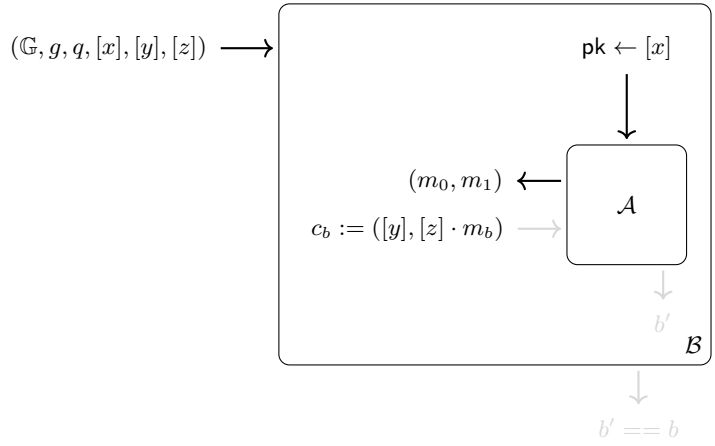
Proof of El Gamal



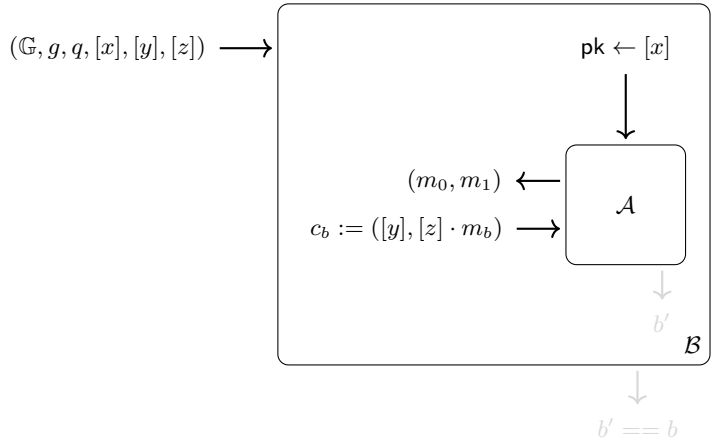
Proof of El Gamal



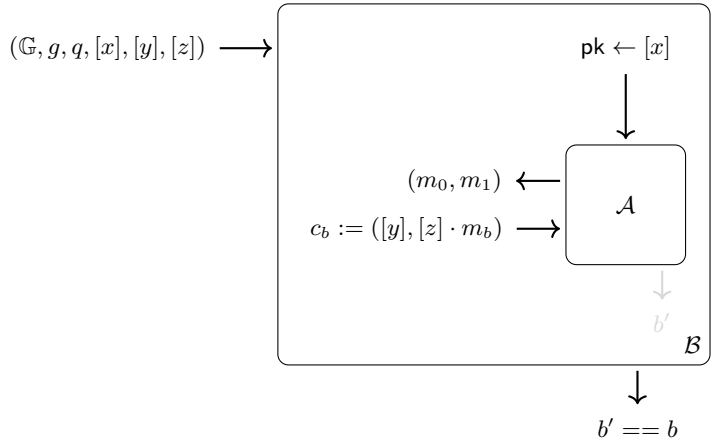
Proof of El Gamal



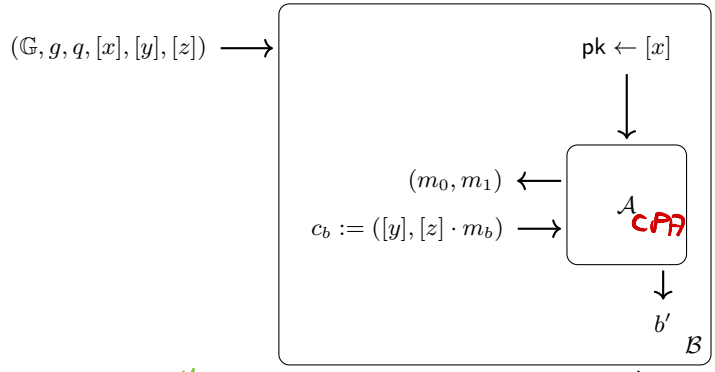
Proof of El Gamal



Proof of El Gamal



Proof of El Gamal



$$\left| \Pr[\mathrm{DDH}(z = xy) = 1] - \Pr[\mathrm{DDH}(z \neq xy) = 1] \right| \leq \mathrm{negl}$$

$$= \left| \tfrac{1}{2} + \text{non-negl} - \tfrac{1}{2} \right| = |\text{non-negl}|$$

Feedback

Your *anonymous feedback* is invaluable to us, and we are truly grateful for your time and insights.

Thank you for helping us improve!

https://tuwel.tuwien.ac.at/mod/feedback/view.php?id=2459258

PRIVACY
ENHANCING
TECHNOLOGIES