

Statistically Secure Sigma Protocols with Abort

Anders Fog Bunzel

Aarhus University

September 16, 2016

Overview

Introduction

- Sigma Protocols
- Security of Sigma Protocols

A Statistically Secure Sigma Protocol

- Setup of Protocol 4.1
- Protocol 4.1
- Theorem 4.2
- Theorem 3.1

Proof of Theorem 4.2

- Statistical Completeness
- Statistical Special Soundness
- Computational sHVZK

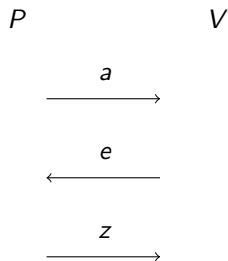
Conclusion

Sigma Protocols

P claims that he know some piece of information such as a secret key to a given public key.

A sigma protocol implies:

- ▶ an identification scheme.
- ▶ a signature scheme.
- ▶ a zero-knowledge protocol.
- ▶ a commitment scheme.



Security of Sigma Protocols

The security of a sigma protocol is based on the hardness of some computational problem such as:

- ▶ Prime factorization: Given $n = p \cdot q$, find the primes p and q .
- ▶ Discrete logarithm: Given $h = g^w \bmod p$, find w .

But, what about lattice problems such as the shortest vector problem (SVP)?

- ▶ Given a lattice \hat{v} , find the shortest vector \vec{v} in \hat{v} .
- ▶ SVP reduces to the problem of finding *small* preimages.
- ▶ And hence, traditionally sigma protocols are insecure when using lattice problems.

Setup of Protocol 4.1 (1/2)

- ▶ A polynomial time bounded prover P and verifier V .
- ▶ An additive homomorphic function $f : (\mathbb{Z}^n, +) \mapsto (G, \circ)$ such that $f(\vec{c} + \vec{d}) = f(\vec{c}) \circ f(\vec{d})$ for all $\vec{c}, \vec{d} \in \mathbb{Z}^n$.
- ▶ The interval $I = [-(S \cdot B - B); S \cdot B - B]$ for $S, B \geq 1$.
- ▶ The witness $\vec{w} \in \mathbb{Z}^n$ for the problem x in the relation R where $\|\vec{w}\|_\infty \leq B$, $x = (f, y)$ and $y = f(\vec{w})$.
- ▶ The commitment scheme commit with public key pk , which comes in two flavors:
 - ▶ Unconditional binding and computational hiding.
 - ▶ Computational binding and perfect hiding.
- ▶ The provers abort probability

$$\Pr[\vec{z} \notin I^n] = 1 - \left(\frac{2 \cdot (S \cdot B - B) + 1}{2 \cdot (S \cdot B) + 1} \right)^n.$$

Setup of Protocol 4.1 (2/2)

- ▶ The limit $E = t \cdot (1 - \Pr[\vec{z} \notin I^n]) - t \cdot \epsilon$ where $\epsilon \in (0; 1]$.
- ▶ The linear secret sharing code $C = [n + \ell, k, d]_q$ that satisfies:
 - ▶ $(d^\perp - \ell - 1)$ -privacy where d^\perp is the minimum distance of the dual code C^\perp .

Massey's LSSS: To secret share $s \in \mathbb{F}_q^\ell$ we choose $c = (c_1, \dots, c_\ell, c_{\ell+1}, \dots, c_{\ell+n}) \in_R C$ such that $s = (c_1, \dots, c_\ell)$ where $(c_{\ell+1}, \dots, c_{\ell+n})$ are the shares of s and $|C| = q^k$. And hence, for Protocol 4.1 we choose:

- ▶ $\ell = 1$ for small codewords
- ▶ a large k to increase the number of codewords
- ▶ an E such that $d > 2 \cdot (t - E)$ where $t = n + \ell$

Protocol 4.1 (1/2)

Prover $P(\vec{w}, x)$

$\vec{r}_i \in_R \mathbb{Z}^n$ such that

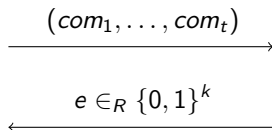
$$\|\vec{r}_i\|_\infty \leq S \cdot B$$

$$a_i = f(\vec{r}_i)$$

$$s_i \in_R \mathbb{Z}$$

$$com_i = \text{commit}_{pk}(a_i, s_i)$$

Verifier $V(x)$



Protocol 4.1 (2/2)

$$c = C(e)$$

$$\vec{z}_i = \vec{r}_i + c \cdot \vec{w}$$

if $\vec{z}_i \in I^n$ then

$$\mathcal{Z}_i = (\vec{z}_i, a_i, s_i)$$

else $\mathcal{Z}_i = \perp$

$$\xrightarrow{(\mathcal{Z}_1, \dots, \mathcal{Z}_t)}$$

$$c = C(e)$$

accept iff at least E :

$$\mathcal{Z}_i \neq \perp,$$

$$\text{com}_i = \text{commit}_{\text{pk}}(a_i, s_i)$$

$$\text{and } f(\vec{z}_i) = a_i \circ y^c$$

Theorem (4.2)

Let $\text{commit}^{ub, ch}$ be an unconditional binding and computational hiding commitment scheme and $\text{commit}^{cb, ph}$ a computational binding and perfect hiding commitment scheme.

Protocol 4.1 satisfies

	$\text{commit}^{ub, ch}$	$\text{commit}^{cb, ph}$
Completeness	Statistical	Statistical
Special soundness	Perfect	Statistical
sHVZK	Computational	Perfect

and hence is a statistically secure sigma protocol.

Theorem (3.1)

Let $\text{commit}^{ub, ch}$ be an unconditional binding and computational hiding commitment scheme and $\text{commit}^{cb, ph}$ a computational binding and perfect hiding commitment scheme.

The general framework with abort (Protocol 3.1) satisfies

	$\text{commit}^{ub, ch}$	$\text{commit}^{cb, ph}$
Completeness	Aborts with prob.	$\Pr[\vec{z} \notin I^n]$
Special soundness	Perfect	Statistical
sHVZK	Computational	Perfect

Proof of Theorem 4.2

Let (P, V) be the general framework with abort and let (P_Σ, V_Σ) be Protocol 4.1.

Statistical Completeness (1/6)

Definition

If P_Σ and V_Σ follows the protocol on input x and private input \vec{w} to P_Σ where $(\vec{w}, x) \in R$, then is the probability that V_Σ outputs reject negligible in t .

Statistical Completeness (2/6)

Proof.

Assume that P_Σ know a witness \vec{w} such that $(\vec{w}, x) \in R$.

We have to prove, that the following limit E implies that V_Σ only rejects P_Σ with probability negligible in t .

$$E = t \cdot (1 - \Pr[\vec{z} \notin I^n]) - t \cdot \epsilon$$

Statistical Completeness (3/6)

A conversation is on the form $(com_i, c, \mathcal{Z}_i)$ for $i = 1, \dots, t$ where:

- ▶ (com_1, \dots, com_t) and $(\mathcal{Z}_1, \dots, \mathcal{Z}_t)$ are fully independent because of the used randomness.
 - ▶ $com_i = \text{commit}_{pk}(a_i, s_i)$
 - ▶ $\mathcal{Z}_i = \perp$ or $\mathcal{Z}_i = (\vec{z}_i, a_i, s_i)$
- ▶ c is only $(d^\perp - 2)$ -wise independent because of the linear secret sharing code C .
 - ▶ $c = C(e)$

Statistical Completeness (4/6)

We can use the Chernoff-Hoeffding bound with limited independence (CHwLI).

1. Let X_i for $i = 1, \dots, t$ denote the conversations where:
 - ▶ $X_i = 1$ if conversation i is an accepting conversation.
 - ▶ $X_i = 0$ otherwise.
2. Define $X = \sum_{i=1}^t X_i$ and $\mu(t) = t \cdot (1 - \Pr[\vec{z} \notin I^n])$.
3. Let $d^\perp = t \cdot \alpha$ for some $\alpha \in [0; 1]$.
4. Define the independence as $\ell(t) = (t \cdot \alpha) - 2$.

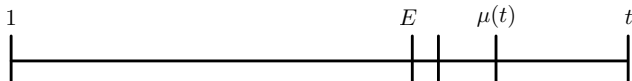
Statistical Completeness (5/6)

CHwLI says that

$$\Pr[|X - \mu(t)| \geq \epsilon \cdot \mu(t)]$$

is negligible in t for any $\ell(t)$ where ϵ is the same as in E .

1. Use CHwLI to argue that X lies between 1 and $\mu(t) - \epsilon \cdot \mu(t)$ with probability negligible in t .
2. Prove that $|E - \mu(t)| \geq \epsilon \cdot \mu(t)$.



Statistical Completeness (6/6)

$$\begin{aligned} |E - \mu(t)| &= |(t \cdot (1 - \Pr[\vec{z} \notin I^n]) - t \cdot \epsilon) - \mu(t)| \\ &= |(\mu(t) - t \cdot \epsilon) - \mu(t)| \\ &= |-t \cdot \epsilon| \\ &= t \cdot \epsilon \\ &\geq \mu(t) \cdot \epsilon \end{aligned}$$



Statistical Special Soundness (1/3)

Definition

Let (com, c, \mathcal{Z}) and (com', c', \mathcal{Z}') be two accepting conversations for the same x where $c \neq c'$. Furthermore, let Ext be a probabilistic polynomial time knowledge extractor. The probability that Ext on input $(x, com, com', c, c', \mathcal{Z}, \mathcal{Z}')$ can't extract a correct witness from the prover is negligible in the length of x .

Statistical Special Soundness (2/3)

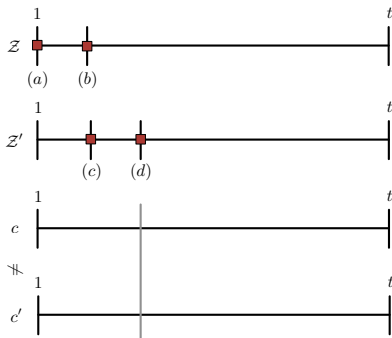
Proof.

Let $com = (com_1, \dots, com_t)$ and $\mathcal{Z} = (\mathcal{Z}_1, \dots, \mathcal{Z}_t)$.

1. Assume that P_Σ can produce two accepting conversations (com, c, \mathcal{Z}) and (com', c', \mathcal{Z}') with different challenges $c \neq c'$ for (P_Σ, V_Σ) .
2. Prove that there exists an index j such that $(com_j, c_j, \mathcal{Z}_j)$ and $(com'_j, c'_j, \mathcal{Z}'_j)$ are two accepting conversations with different challenges $c_j \neq c'_j$ for (P, V) .
3. Since (P, V) satisfies statistical special soundness, we have that (P_Σ, V_Σ) also satisfies this property.

Statistical Special Soundness (3/3)

- ▶ At most $t - E$ aborting conversations.
- ▶ $\mathcal{Z}_i = \perp$ for all i between point (a) and (b).
- ▶ $\mathcal{Z}'_i = \perp$ for all i between point (c) and (d).
- ▶ Make sure that $\Delta(c, c') > 2 \cdot (t - E)$ for all $c, c' \in \mathcal{C}$ by choosing $d > 2 \cdot (t - E)$.



Computational sHVZK

Definition

There exists a probabilistic polynomial time simulator Sim , which on input x and a random challenge c , outputs an accepting conversation (com, c, \mathcal{Z}) such that $\text{Sim}(x, c) \sim^c (P_{\Sigma}(\vec{w}), V_{\Sigma})(x)$.

Proof.

Since (P, V) satisfies computational sHVZK, we have that (P_{Σ}, V_{Σ}) also satisfies this property because sHVZK is invariant under parallel composition.



Conclusion

We have constructed a *statistically secure sigma protocol* that satisfies:

	$\text{commit}^{ub,ch}$	$\text{commit}^{cb,ph}$
Completeness	Statistical	Statistical
Special soundness	Perfect	Statistical
sHVZK	Computational	Perfect

and where we can base the security on:

- ▶ The prime factorization problem.
- ▶ The discrete logarithm problem.
- ▶ Lattice problems such as the shortest vector problem.