KryptonIT: The Discovery of a New Cryptographic System for Storing Secrets

Reto E. Koenig

University of Fribourg
&
Bern University of Applied Sciences

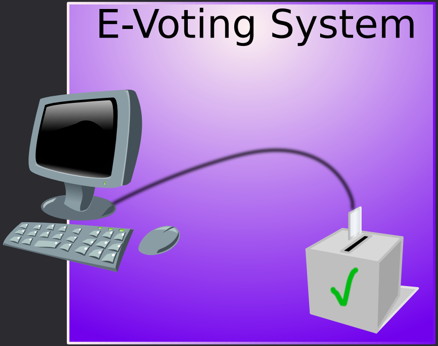
25.03.2011

UNIVERSITAS FRIBURGENSIS
Berner Fachhochschule
HASLERSTIFTUNG

What you should know about building new cryptographic systems

Ronald Rivest: “Never build your own cryptographic system!”

Current E-Voting Systems



Voter's view on a current E-Voting Systems

- It is Understandable
- It is Simple to Use
- Fast
- "Cheap"

Adversary's view on a current E-Voting Systems

Do not Underestimate the Power of the Coercer

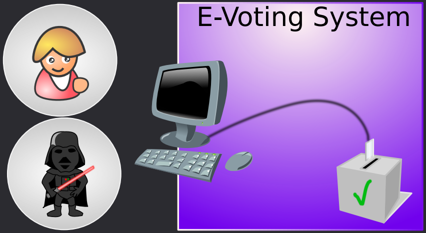
- You Shall Not Vote
- You Shall Vote
- You Shall Vote As I Say
- I randomize Your Vote
- I Vote for You

- I am Watching You
- I Know How You Voted Last Summer

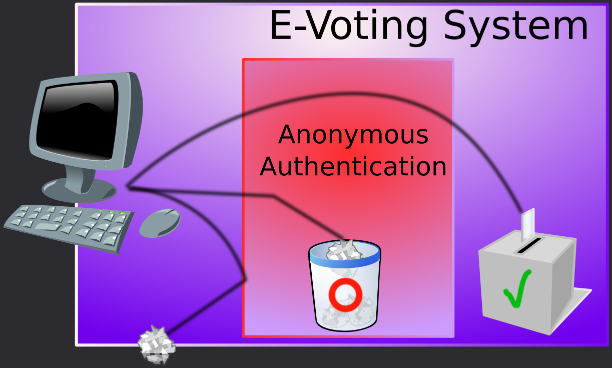
- It is Fast
- It is Scalable
- It is "Cheap"

Overall view on a current E-Voting Systems

- It is Simple
- It is Fast
- It is Cheap
- It is completely insecure



Cryptographer's new Hope



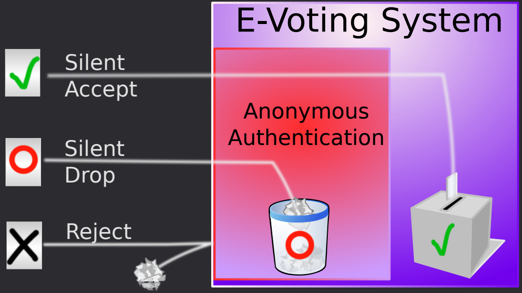
Cryptographer's view on their E-Voting Systems

- It is Coercion-Resistant
- It is End-To-End Verifiable
- It is secure
- The voter has to remember “some” “secrets”

Some Secrets?

E2E verifiable coercion resistant E-Voting systems require:

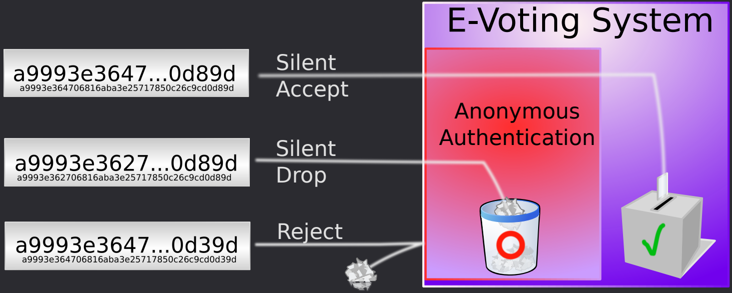
- 3 - different kind of credentials with very high entropy
- kept top secret by each voter



Some Secrets?

E2E verifiable coercion resistant E-Voting systems require:

- 3 - different kind of credentials with very high entropy
- kept top secret by each voter



A Realistic Example With 20 Credentials

In order to render the E-Voting System coercion resistant, each voter...

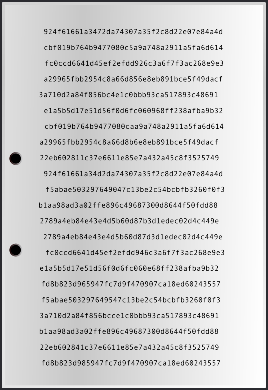
- ...needs to secretly store several dozens credentials
- ...has to discriminate doubtless between credentials for 'Accept' and 'Drop'.[a]
- ...is not allowed to mark any credential
- ...shall never unveil the amount of possessed secrets (They vary per voter)

[a] E-voting system accepts both without returning any hint

A Realistic Example With 20 Credentials

In order to render the E-Voting System coercion resistant, each voter...

- ...needs to secretly store several dozens credentials
- ...has to discriminate doubtless between credentials for 'Accept' and 'Drop'.[a]
- ...is not allowed to mark any credential
- ...shall never unveil the amount of possessed secrets (They vary per voter)



[a] E-voting system accepts both without returning any hint

A Realistic Example With 20 Credentials

In order to render the E-Voting System coercion resistant, each voter...

- ...needs to secretly store several dozens credentials
- ...has to discriminate doubtless between credentials for 'Accept' and 'Drop'.[a]
- ...is not allowed to mark any credential
- ...shall never unveil the amount of possessed secrets (They vary per voter)

[a] E-voting system accepts both without returning any hint

But How Should the Voter Store those Secrets?

Indeed it is not possible to store these secrets with some keys (passwords) in a current crypto-systems. ($\rightarrow$ Discussion)

Our View on the Secret-Storage System

The system...

- ...allows to choose freely n (usually low entropy) keys
- ...allows to choose freely n (usually high entropy) secrets
- ...has to store multiple secrets in one storage (aka cipher)
- ...has to retrieve only the secret correlated to the key
- ...has to have all properties of a (symmetric) crypto-system

Let's get Formal...

Prerequisits

$\mathcal{S}$ $=$*secret space*, set of all possible secrets (typically high-entropy)

$\mathcal{K}$ $=$*key space*, set of all possible keys (typically low-entropy)

S $= (s_1, \ldots, s_n)$, $s_i \in \mathcal{S}$, an n-tuple of (not necessarily distinct) secrets ($n \geq 1$)

K $= (k_1, \ldots, k_n)$, $k_i \in \mathcal{K}$, an n-tuple of distinct keys $n \geq 1$

$\mathcal{C}$ $=$*storage space*, the set of all possible storages

c $=$a particular storage

Functions of the Secret-Storing System

$$\text{store}: \mathcal{S}^n \times \mathcal{K}^{(n)} \longrightarrow \mathcal{C}$$

storage function, where $\mathcal{K}^{(n)} \subseteq \mathcal{K}^n$ is the set of all admissible key tuples (with distinct keys)

$$\text{retrieve}: \mathcal{C} \times \mathcal{K} \longrightarrow \mathcal{S}$$

the *retrieval function*

$\text{store}_K(S) =$ $c \in \mathcal{C}$, storing the n-tuple of the secrets $S \in \mathcal{S}^n$ with the n-tuple of distinct keys $K \in \mathcal{K}^{(n)}$

$\text{retrieve}_{k_i}(c) =$ $s_i \in \mathcal{S}$ retrieval with key k_i

---

$$\text{retrieve}_{k_i}(\text{store}_K(S)) = s_i$$

Properties of the Secret-Stroring System

Required to possess the cryptographic properties of a traditional symmetric crypto-system:

- Retrieving s_i from c does not disclose any information about the other secrets in c
- Applying K on c returns S
- Serves a conditional entropy $H(S|c)$ which is equal to $H(S)$
- Applying K' on c where $K' \neq K$ does return S with a probability of $\frac{1}{|S|}$

Definition

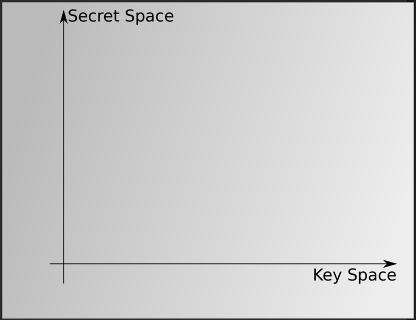
A *secret-storing system* of order n,

$$\Sigma = (\mathcal{S}, \mathcal{K}, \mathcal{C}, \mathsf{store}, \mathsf{retrieve}),$$

consists of a secret space $\mathcal{S}$, a key space $\mathcal{K}$, a storage space $\mathcal{C}$, and two functions store and retrieve with properties as introduced above.

An Example in $\mathbb{R}$ (Storing)

$$S = (s_1, \dots, s_i, \dots, s_n)$$
$$K = (k_1, \dots, k_i, \dots, k_n)$$
$$c = \mathrm{store}_K(S)$$
$$c = \Lambda^*_K(S)$$
$$c = f = \sum_{z=0}^{t} a_z x^z$$



*Lagrange interpolation

An Example in $\mathbb{R}$ (Storing)

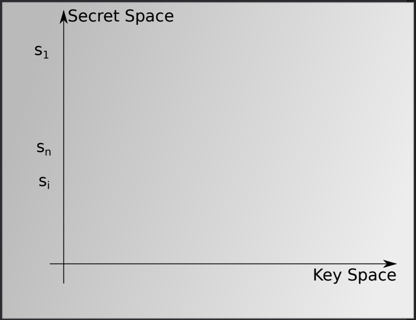
$S = (s_1, \ldots, s_i, \ldots, s_n)$

$K = (k_1, \ldots, k_i, \ldots, k_n)$

$c = \text{store}_K(S)$

$c = \Lambda^*_K(S)$

$c = f = \sum_{z=0}^{t} a_z x^z$



*Lagrange interpolation

An Example in $\mathbb{R}$ (Storing)

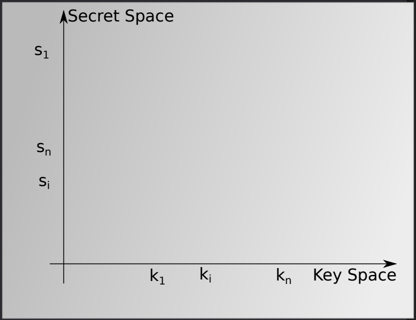
$S = (s_1, \ldots, s_i, \ldots, s_n)$

$K = (k_1, \ldots, k_i, \ldots, k_n)$

$c = \text{store}_K(S)$

$c = \Lambda^*_K(S)$

$c = f = \sum_{z=0}^{t} a_z x^z$

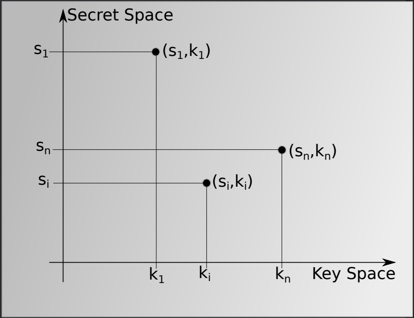


---

*Lagrange interpolation

An Example in $\mathbb{R}$ (Storing)

$S = (s_1, \ldots, s_i, \ldots, s_n)$
$K = (k_1, \ldots, k_i, \ldots, k_n)$
$c = \text{store}_K(S)$
$c = \Lambda^*_K(S)$
$c = f = \sum_{z=0}^{t} a_z x^z$



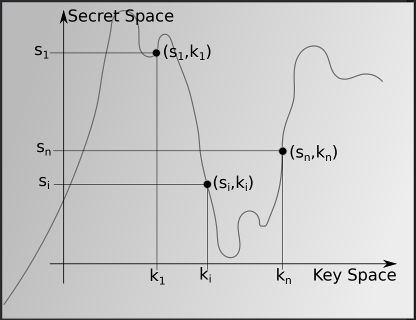
---

*Lagrange interpolation

An Example in $\mathbb{R}$ (Storing)

$S = (s_1, \ldots, s_i, \ldots, s_n)$
$K = (k_1, \ldots, k_i, \ldots, k_n)$
$c = \text{store}_K(S)$
$c = \Lambda^*_K(S)$

$$c = f = \sum_{z=0}^{t} a_z x^z$$

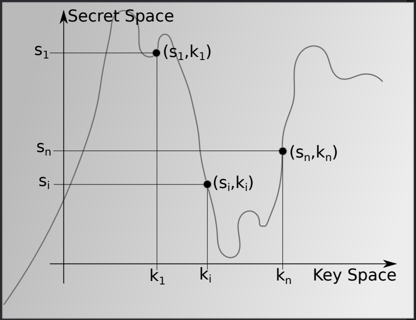


*Lagrange interpolation

An Example in $\mathbb{R}$ (Storing)

$$S = (s_1, \ldots, s_i, \ldots, s_n)$$
$$K = (k_1, \ldots, k_i, \ldots, k_n)$$
$$c = \text{store}_K(S)$$
$$c = \Lambda^*_K(S)$$
$$c = f = \sum_{z=0}^{t} a_z x^z$$

*Lagrange interpolation

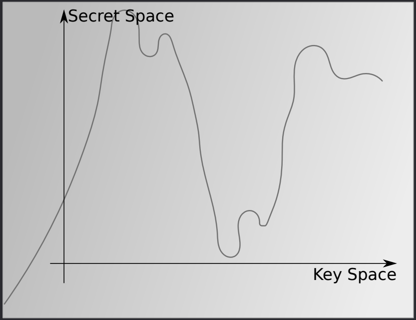


An Example in $\mathbb{R}^2$ (Retrieving)

$$c = f = \sum_{z=0}^{t} a_z x^z$$

$$s_i = \text{retrieve}_{k_i}(c)$$

$$s_i = f(k_i) = \sum_{z=0}^{t} a_z {k_i}^z$$

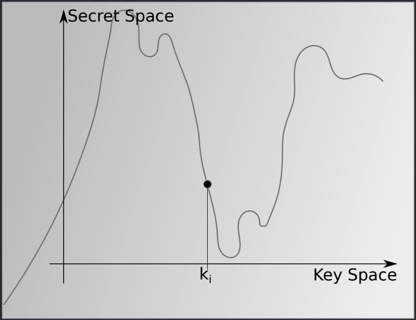


An Example in $\mathbb{R}^2$ (Retrieving)

$$c = f = \sum_{z=0}^{t} a_z x^z$$

$$s_i = \text{retrieve}_{k_i}(c)$$

$$s_i = f(k_i) = \sum_{z=0}^{t} a_z {k_i}^z$$

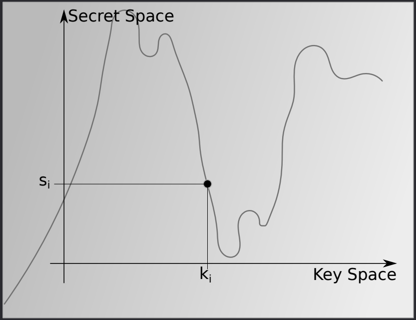


An Example in $\mathbb{R}^2$ (Retrieving)

$$c = f = \sum_{z=0}^{t} a_z x^z$$

$$s_i = \text{retrieve}_{k_i}(c)$$

$$s_i = f(k_i) = \sum_{z=0}^{t} a_z {k_i}^z$$



Considerations

Cryptographers do not like $\mathbb{R}$... too chatty... too dense

The secret-storing system hence is created in a Galois field $\mathbb{F}_p$

Problems:

Considerations

Cryptographers do not like $\mathbb{R}$... too chatty... too dense
The secret-storing system hence is created in a Galois field $\mathbb{F}_p$

Problems:

- How can the user be free in its choice of k if the field $\mathbb{F}_p$ is finite?
- How can the secret space $|S|$ be reduced / how can $\mathbb{F}_p$ be made 2^k times greater than $|S|$? ($k \approx 100$)

Considerations

Cryptographers do not like $\mathbb{R}$... too chatty... too dense
The secret-storing system hence is created in a Galois field $\mathbb{F}_p$

Problems:

- How can the user be free in its choice of k if the field $\mathbb{F}_p$ is finite?
- How can the secret space $|S|$ be reduced / how can $\mathbb{F}_p$ be made 2^k times greater than $|S|$? ($k \approx 100$)

Considerations

Cryptographers do not like $\mathbb{R}$... too chatty... too dense
The secret-storing system hence is created in a Galois field $\mathbb{F}_p$

Problems:

- How can the user be free in its choice of k if the field $\mathbb{F}_p$ is finite?
- How can the secret space $|\mathcal{S}|$ be reduced / how can $\mathbb{F}_p$ be made 2^k times greater than $|S|$? ($k \approx 100$)

Considerations

Problems:

- How can the user be free in its choice of k if the field $\mathbb{F}_p$ is finite?
- How can the secret space $|\mathcal{S}|$ be reduced / how can $\mathbb{F}_p$ be made 2^k times greater than $|S|$? ($k \approx 100$)

Solution:

Use a collision free mapping function per storage:

$\varkappa_K(k_0) : K \mapsto K', k_0 \in \mathbb{Z}, k_i' \in \mathbb{F}_p \forall k_i' \in K', |K| = |K'|$

$\varkappa_{k_i}(k_0) : k_i \mapsto k_i', k_0 \in \mathbb{Z}, k_i \in K, k_i' \in K'$

The secret c now consists of the two-tuple (f, k_0)

Considerations

Problems:

- How can the user be free in its choice of k if the field $\mathbb{F}_p$ is finite?
- How can the secret space $|\mathcal{S}|$ be reduced / how can $\mathbb{F}_p$ be made 2^k times greater than $|S|$? ($k \approx 100$)

Solution:

Use a collision free mapping function per storage:

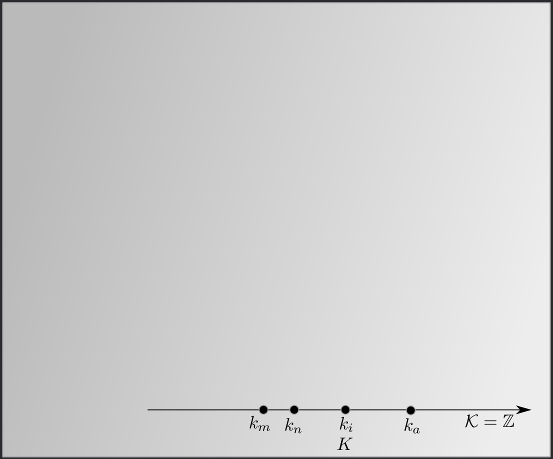
$\varkappa_K(k_0) : K \mapsto K', k_0 \in \mathbb{Z}, k'_i \in \mathbb{F}_p \forall k'_i \in K', |K| = |K'|$

$\varkappa_{k_i}(k_0) : k_i \mapsto k'_i, k_0 \in \mathbb{Z}, k_i \in K, k'_i \in K'$

The secret c now consists of the two-tuple (f, k_0)

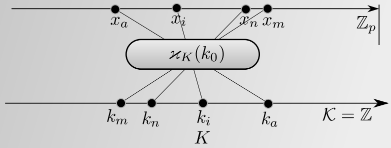
Considerations: Enhancing the Key Space

Use a collision free mapping function per storage $\varkappa_K(k_0)$



Considerations: Enhancing the Key Space

Use a collision free mapping function per storage $\varkappa_K(k_0)$



Considerations

Problems:

- How can the user be free in its choice of k if the field $\mathbb{F}_p$ is finite?
- How can the secret space $|\mathcal{S}|$ be reduced / how can $\mathbb{F}_p$ be made 2^k times greater than $|\mathcal{S}|$? ($k \approx 100$)

Solution:

Use a function $\varsigma : \mathbb{Z}_p \mapsto \mathcal{S}$ where ς^{-1} is surjective and easy to calculate:

$\varsigma := s_i \equiv y_i \mod |\mathcal{S}|$, where $y_i = f(k')$

$\varsigma^{-1} := y_i = s_i + q \times |\mathcal{S}|, q \in_R \mathbb{N}, y_i < p$

Considerations

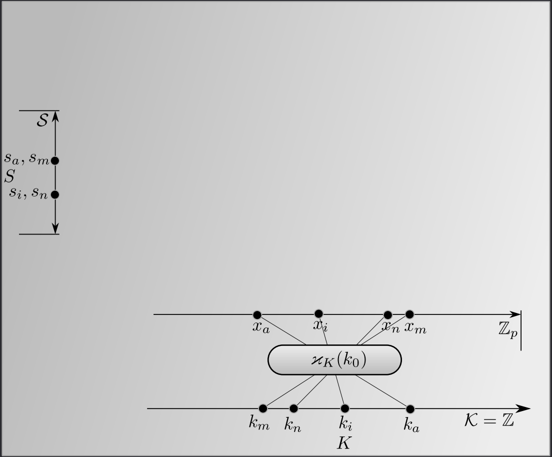
Problems:

- How can the user be free in its choice of k if the field $\mathbb{F}_p$ is finite?
- How can the secret space $|\mathcal{S}|$ be reduced / how can $\mathbb{F}_p$ be made 2^k times greater than $|\mathcal{S}|$? ($k \approx 100$)

Solution:
Use a function $\varsigma : \mathbb{Z}_p \mapsto \mathcal{S}$ where ς^{-1} is surjective and easy to calculate:
$\varsigma := s_i \equiv y_i \mod |\mathcal{S}|$, where $y_i = f(k')$
$\varsigma^{-1} := y_i = s_i + q \times |\mathcal{S}|, q \in_R \mathbb{N}, y_i < p$

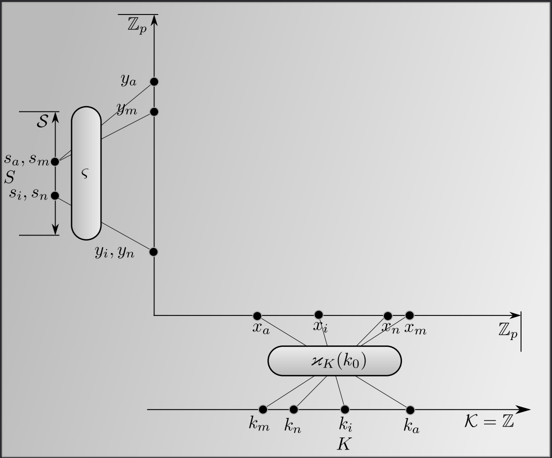
Considerations: Reducing the Secret Space

Use a function $\varsigma : \mathbb{Z}_p \mapsto \mathcal{S}$



Considerations: Reducing the Secret Space

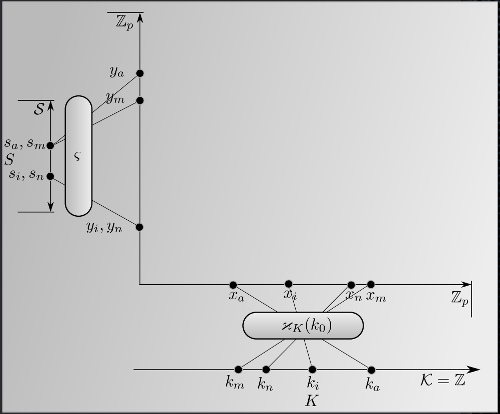
Use a function $\varsigma : \mathbb{Z}_p \mapsto \mathcal{S}$



Considerations

$$S = (s_1, \ldots, s_i, \ldots, s_n)$$
$$K = (k_1, \ldots, k_i, \ldots, k_n)$$
$$c = \mathrm{store}_K(S)$$
$$K' = \varkappa_K(k_0)$$
$$S' = \varsigma^{-1}(S)$$
$$f = \Lambda_{K'}(S')$$
$$c = (f, k_0)$$

$$s_i = \mathrm{retrieve}_{k_i}(c)$$
$$k_i' = \varkappa_{k_i}(k_0)$$
$$s_i' = f(k_i')$$
$$s_i = \varsigma(s_i')$$



Considerations

$S = (s_1, \ldots, s_i, \ldots, s_n)$

$K = (k_1, \ldots, k_i, \ldots, k_n)$

$c = \text{store}_K(S)$

$K' = \varkappa_K(k_0)$

$S' = \varsigma^{-1}(S)$

$f = \Lambda_{K'}(S')$

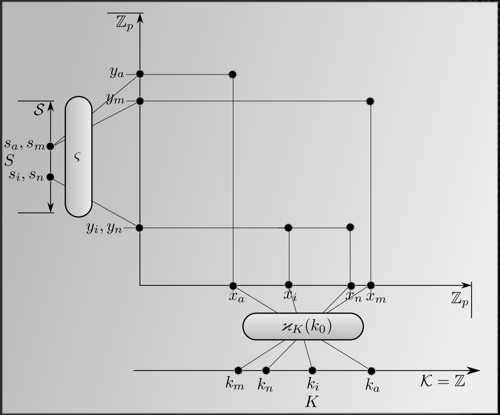
$c = (f, k_0)$

$s_i = \text{retrieve}_{k_i}(c)$

$k'_i = \varkappa_{k_i}(k_0)$

$s'_i = f(k'_i)$

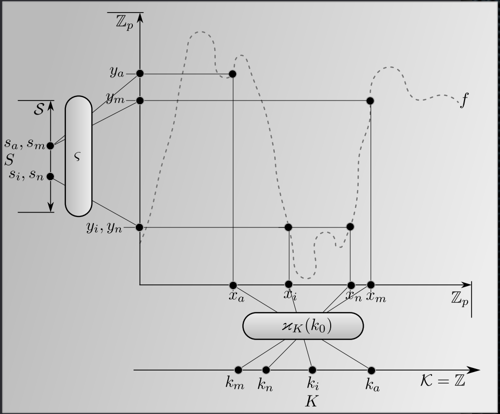
$s_i = \varsigma(s'_i)$



Considerations

$$S = (s_1, \dots, s_i, \dots, s_n)$$
$$K = (k_1, \dots, k_i, \dots, k_n)$$
$$c = \text{store}_K(S)$$
$$K' = \varkappa_K(k_0)$$
$$S' = \varsigma^{-1}(S)$$
$$f = \Lambda_{K'}(S')$$
$$c = (f, k_0)$$

$$s_i = \text{retrieve}_{k_i}(c)$$
$$k'_i = \varkappa_{k_i}(k_0)$$
$$s'_i = f(k'_i)$$
$$s_i = \varsigma(s'_i)$$



Considerations

$S = (s_1, \ldots, s_i, \ldots, s_n)$

$K = (k_1, \ldots, k_i, \ldots, k_n)$

$c = \mathrm{store}_K(S)$

$K' = \varkappa_K(k_0)$

$S' = \varsigma^{-1}(S)$

$f = \Lambda_{K'}(S')$

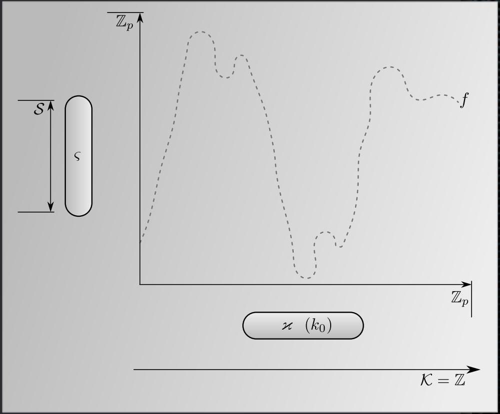
$c = (f, k_0)$

$s_i = \mathrm{retrieve}_{k_i}(c)$

$k'_i = \varkappa_{k_i}(k_0)$

$s'_i = f(k'_i)$

$s_i = \varsigma(s'_i)$



Considerations

$S = (s_1, \ldots, s_i, \ldots, s_n)$

$K = (k_1, \ldots, k_i, \ldots, k_n)$

$c = \mathrm{store}_K(S)$

$K' = \varkappa_K(k_0)$

$S' = \varsigma^{-1}(S)$

$f = \Lambda_{K'}(S')$

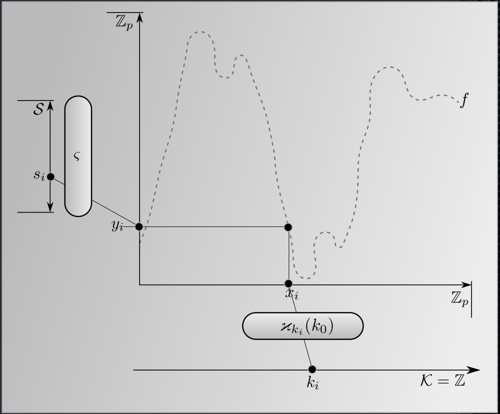
$c = (f, k_0)$

$s_i = \mathrm{retrieve}_{k_i}(c)$

$k'_i = \varkappa_{k_i}(k_0)$

$s'_i = f(k'_i)$

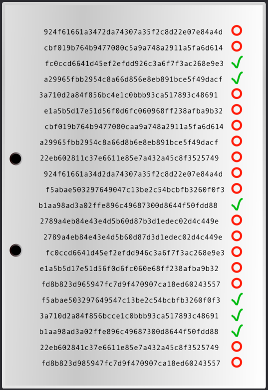
$s_i = \varsigma(s'_i)$



How to Use It For the 20-Credentials

A simple example (it works, but...)

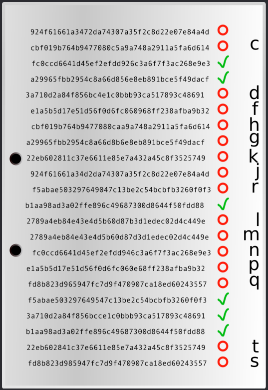
- ...use consonants as keys for the 'Drop' credentials
- ...use vowels as keys for 'Accept' credentials
- ...use some other keys for some credentials
- ...store them in the secret-storage system



How to Use It For the 20-Credentials

A simple example (it works, but...)

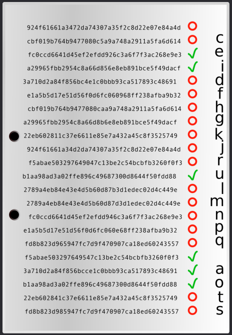
- ...use consonants as keys for the 'Drop' credentials
- ...use vowels as keys for 'Accept' credentials
- ...use some other keys for some credentials
- ...store them in the secret-storage system



How to Use It For the 20-Credentials

A simple example (it works, but...)

- ...use consonants as keys for the 'Drop' credentials
- ...use vowels as keys for 'Accept' credentials
- ...use some other keys for some credentials
- ...store them in the secret-storage system



How to Use It For the 20-Credentials

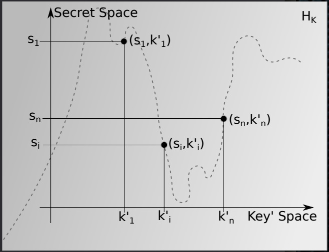
A simple example (it works, but...)

- ...use consonants as keys for the 'Drop' credentials
- ...use vowels as keys for 'Accept' credentials
- ...use some other keys for some credentials
- ...store them in the secret-storage system

How to Use It For the 20-Credentials

A simple example (it works, but...)

- ...use consonants as keys for the 'Drop' credentials
- ...use vowels as keys for 'Accept' credentials
- ...use some other keys for some credentials
- ...store them in the secret-storage system



The secret-storing system brings other very desirable features:

Typoo Resistance via Secret-Storing System | The OR-Function

Either key_i OR key_n unveils the single secret

$s_i = \text{retrieve}_{k_i}(c)$

$s_n = \text{retrieve}_{k_n}(c)$

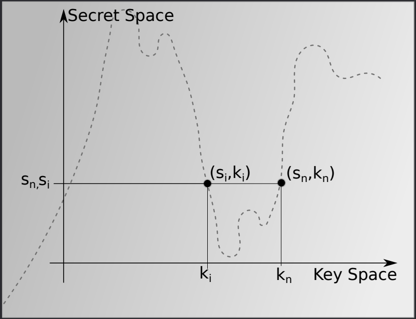
$verify(s_i = s_n)$

The secret-storing system brings other very desirable features:

Typoo Resistance via Secret-Storing System | The OR-Function

Either key_i OR key_n unveils the single secret

$$s_i = \text{retrieve}_{k_i}(c)$$
$$s_n = \text{retrieve}_{k_n}(c)$$
$$verify(s_i = s_n)$$



Key-Hinting via Secret-Storing System | The AND Function

Only key_i AND key_n unveil the single secret:

k_a	"HintMeWith...:"	s_a	"098z71adf4383498"
k_b	"GoodCredentials"	s_b	"aer9393fads932sv3"
k_c	"BadCredentials"	s_c	"598nnja2devm24v3a"
k_d	$s_a \oplus s_b$	s_d	"vowel"
k_e	$s_a \oplus s_c$	s_e	"consonant"

This still is secure as long as the keys carries some entropy!
It is definitely more secure than "What is your mother's maiden name" used nowadays!

And this one for free:

Secret-Sharing via Secret-Storing System | The THRESHOLD Function

Only n out of m keys unveil the single secret...

k_a	"Chief-1"	s_a	"098z71adf4383498"
k_b	"Chief-2"	s_b	"1gfnasdfrhhsadfn"
k_c	"Chief-3"	s_c	"fgjn439f3j22tj93"
k_x	$s_a \oplus s_b$	s_x	"We are bankrupt"
k_y	$s_a \oplus s_c$	s_y	"We are bankrupt"
k_z	$s_b \oplus s_c$	s_z	"We are bankrupt"

Randomized Secret-Storing System

If some sample positions $rx_j \notin K$ are chosen arbitrary with arbitrary sample values ry_j ($R = m$-tuple(rx, ry)), the system changes from a deterministic secret-storing system into a randomized secrets-storing System, where two stores containing the same (K, S) 'look' completely different.

Definition

A *randomized secret-storing system* of order n,

$$\Gamma = (\mathcal{S}, \mathcal{K}, \mathcal{R}, \mathcal{C}, \text{randomStore}, \text{retrieve}),$$

consists of a secret space $\mathcal{S}$, a key space $\mathcal{K}$, a randomization space $\mathcal{R}$, a storage space $\mathcal{C}$, and two functions randomStore and retrieve with properties as introduced above.

Randomized Secret-Storing System

If some sample positions $rx_j \notin K$ are chosen arbitrary with arbitrary sample values ry_j ($R = m$-tuple(rx, ry)), the system changes from a deterministic secret-storing system into a randomized secrets-storing System, where two stores containing the same (K, S) 'look' completely different.

Definition

A *randomized secret-storing system* of order n,

$$\Gamma = (\mathcal{S}, \mathcal{K}, \mathcal{R}, \mathcal{C}, \text{randomStore}, \text{retrieve}),$$

consists of a secret space $\mathcal{S}$, a key space $\mathcal{K}$, a randomization space $\mathcal{R}$, a storage space $\mathcal{C}$, and two functions randomStore and retrieve with properties as introduced above.

The Thing is a Beast

Ring-homomorphism

Every operation (+,*) can be applied using multiple secret-stores as operands. The same operations will then be applied on all secrets of the same key.

This is exactly the most desired feature for a secure* and private* web-service* in the cloud* on the internet* .

A CPU in the cloud can now do calculations using secret-stores, hence not knowing the operands nor the result.

*Bingo ;-)

The Thing is a Beast

Ring-homomorphism

Every operation (+,*) can be applied using multiple secret-stores as operands. The same operations will then be applied on all secrets of the same key.

This is exactly the most desired feature for a secure* and private* web-service* in the cloud* on the internet* .

A CPU in the cloud can now do calculations using secret-stores, hence not knowing the operands nor the result.

*Bingo ;-)

Discussion

This is left as an exercise for the reader...

...One more Thing...

The Asymmetric variant of the secret-storing system with the same properties as shown above.

Please feel Free to Break the Secret-Storing System!

As it is a rather easy concept (even for a young math-student), it is easy to understand the system and thus to look for the show-stopper.... So, if you ever... Please let me know too!

Happy Hacking!