Cryptographic Reverse Firewall via Malleable Smooth Projective Hash Functions

Rongmao Chen, Yi Mu, **Guomin Yang**, Willy Susilo, Fuchun Guo and Mingwu Zhang

UNIVERSITY OF WOLLONGONG AUSTRALIA

国防科學技術大學
National University of Defense Technology

湖北工業大學
HUBEI UNIVERSITY OF TECHNOLOGY

Asiacrypt 2016, Hanoi

Outline

- Background
- Cryptographic Reverse Firewall
- Part I: Malleable Smooth Projective Hash Function
- Part II: CRF Constructions Via Malleable SPHFs
  - Unkeyed Message Transmission Protocol
  - Oblivious Signature-Based Envelope Protocol
  - Oblivious Transfer Protocol
- Conclusions and Future Work

Outline

- **Background**
- **Cryptographic Reverse Firewall**
- **Part I: Malleable Smooth Projective Hash Function**
- **Part II: CRF Constructions Via Malleable SPHFs**
  - **Unkeyed Message Transmission Protocol**
  - **Oblivious Signature-Based Envelope Protocol**
  - **Oblivious Transfer Protocol**
- **Conclusions and Future Work**

Background

- Edward Snowden Revelations
- Massive surveillance by intelligence agencies
- Undermining security mechanisms ☹
  - subverting cryptographic protocols
  - deploying security weakness in implementations

Background

- Edward Snowden Revelations
- Massive surveillance by intelligence agencies
- Undermining security mechanisms ☹
  - subverting cryptographic protocols
  - deploying security weakness in implementations
- **Post-Snowden Cryptography ☺**
  - How to achieve meaningful security for cryptographic protocols in the presence of an adversary that may arbitrarily tamper with the victim's machine?

IACR Statement On Mass Surveillance

The membership of the IACR repudiates mass surveillance and the undermining of cryptographic solutions and standards, Population-wide surveillance threatens democracy and human dignity. We call for expediting research and deployment of effective techniques to protect personal privacy against governmental and corporate overreach.

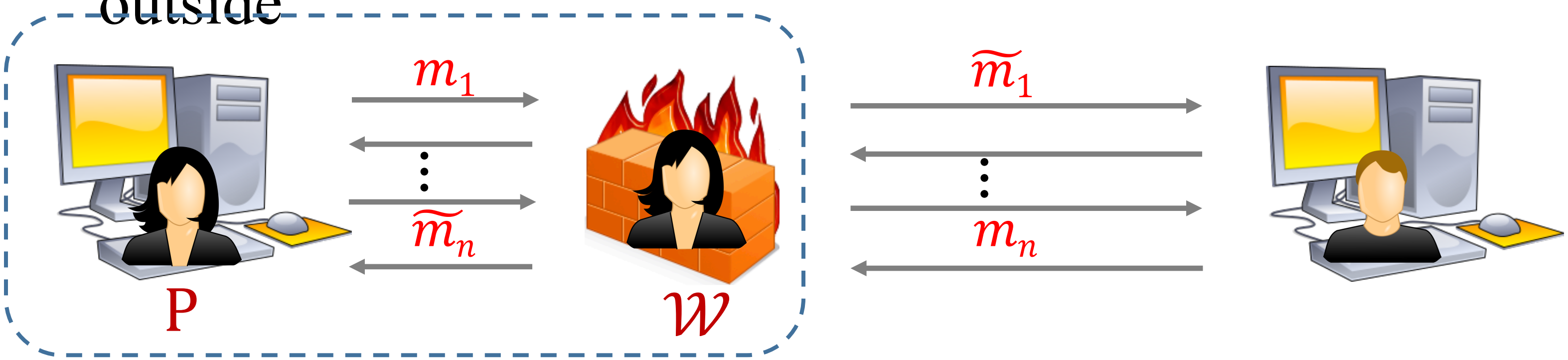
--Copenhagen, Eurocrypt 2014

Outline

- Background
- **Cryptographic Reverse Firewall**
- Part I: Malleable Smooth Projective Hash Function
- Part II: CRF Constructions Via Malleable SPHFs
  - Unkeyed Message Transmission Protocol
  - Oblivious Signature-Based Envelope Protocol
  - Oblivious Transfer Protocol
- Conclusions and Future Work

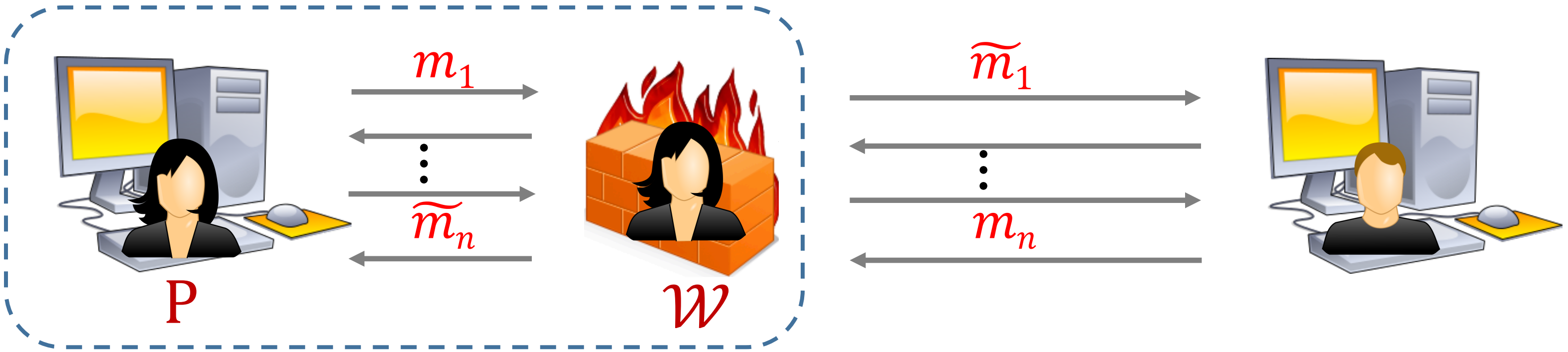
Cryptographic Reverse Firewall [MS15]

- A *stateful* algorithm $\mathcal{W}$
  - Input: current state τ and message m
  - Output: updated state $\tilde{\tau}$ and message $\widetilde{m}$
- A *"composed"* party $\mathcal{W} \circ \mathrm{P}$
  - $\mathcal{W}$ is applied to the incoming and outgoing messages of party P
  - the state of $\mathcal{W}$ is initialized to the public parameters
  - $\mathcal{W}$ is called a reverse firewall for P
  - "active router" between P 's private network and the outside



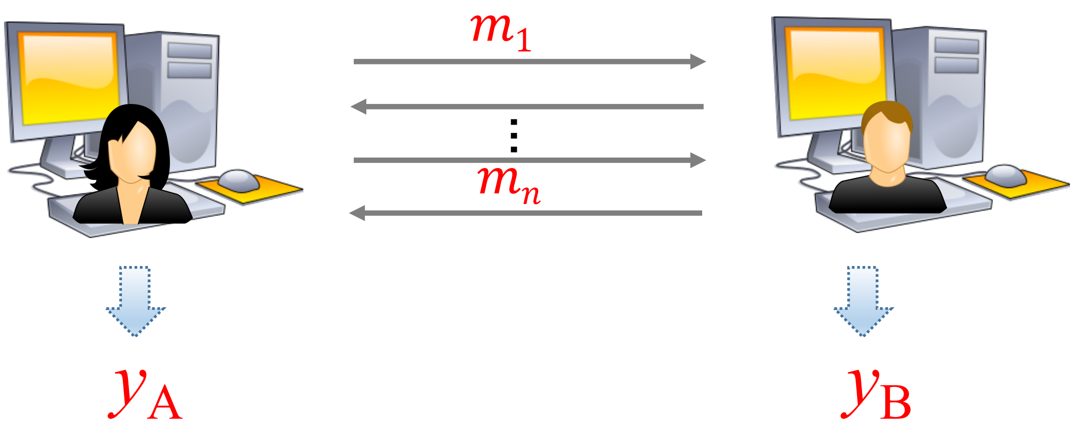
Cryptographic Reverse Firewall [MS15]

- *Stackable* reverse firewalls
  - composition of multiple reverse firewalls $\mathcal{W} \circ \mathcal{W} \circ \cdots \circ \mathcal{W} \circ \mathrm{P}$
- *Transparent* to legitimate traffic
  - does not break functionality ***(Functionality-maintaining)***
- $\mathcal{W}$ shares *no* secret with P
  - we do not trust the firewall ***(Security-preserving)***
- *No* corrupted implementation of P can leak information through $\mathcal{W}$ ***(Exfiltration-resistant)***

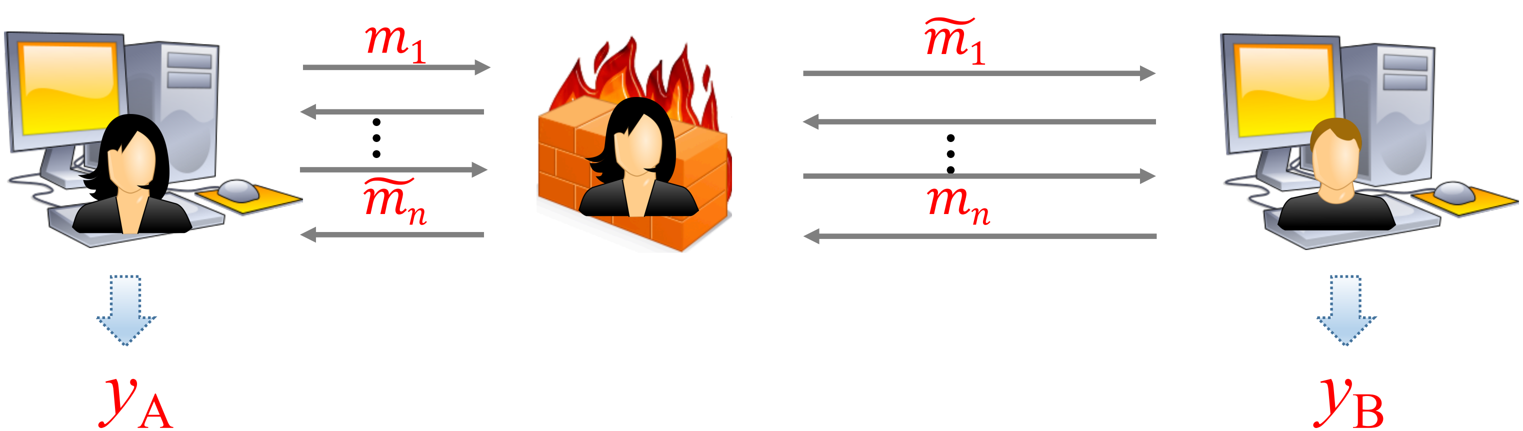


Property I: Functionality-Maintaining

- Underlying protocol has some *functionality*

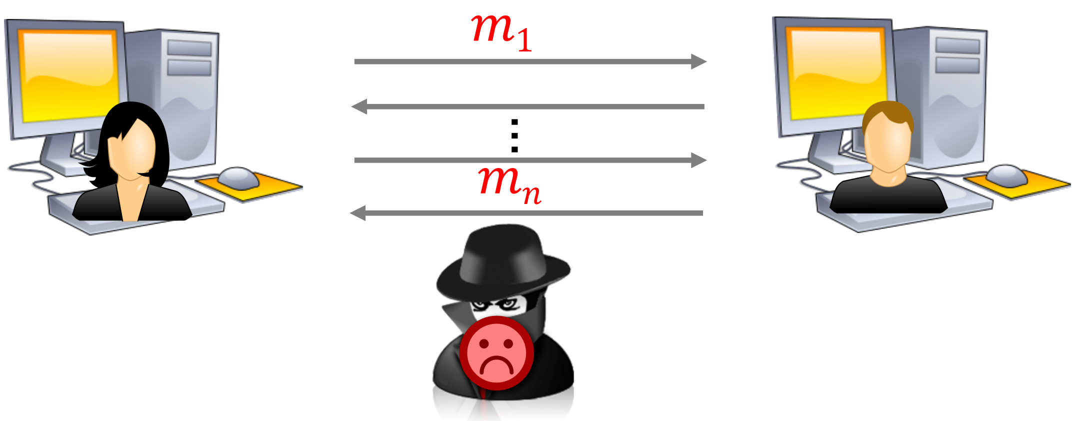


- Protocol with $\mathcal{W}$ has the same *functionality*

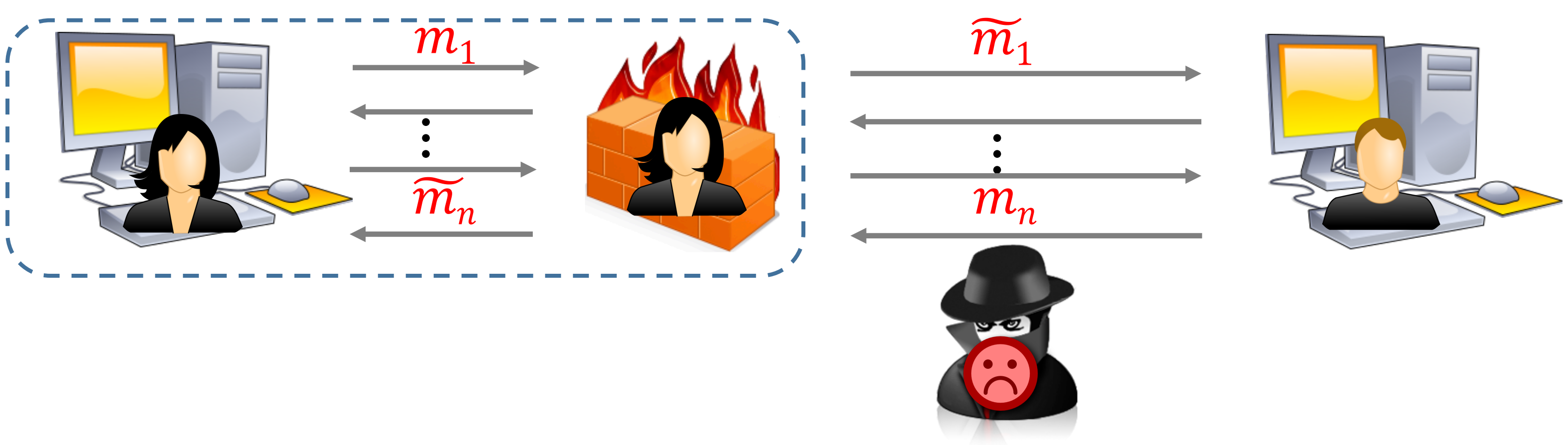


Property II: Security-Preserving

- Underlying protocol satisfies some *security notions*

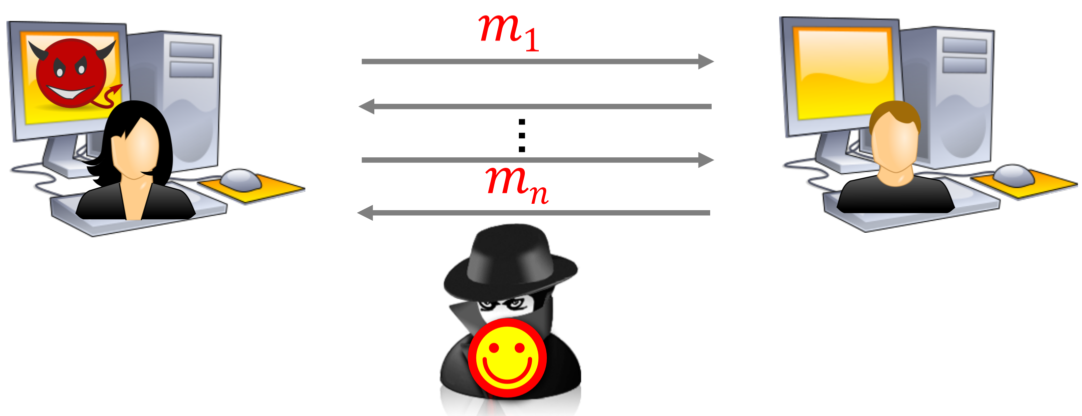


- Protocol with $\mathcal{W}$ satisfies the same *security notions*

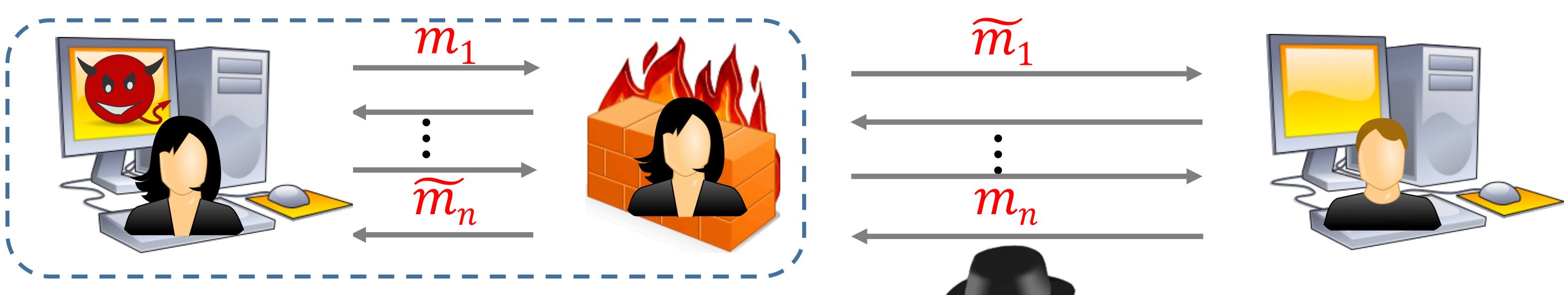


Property II: Security-Preserving

- Corrupted implementation may *break* the security



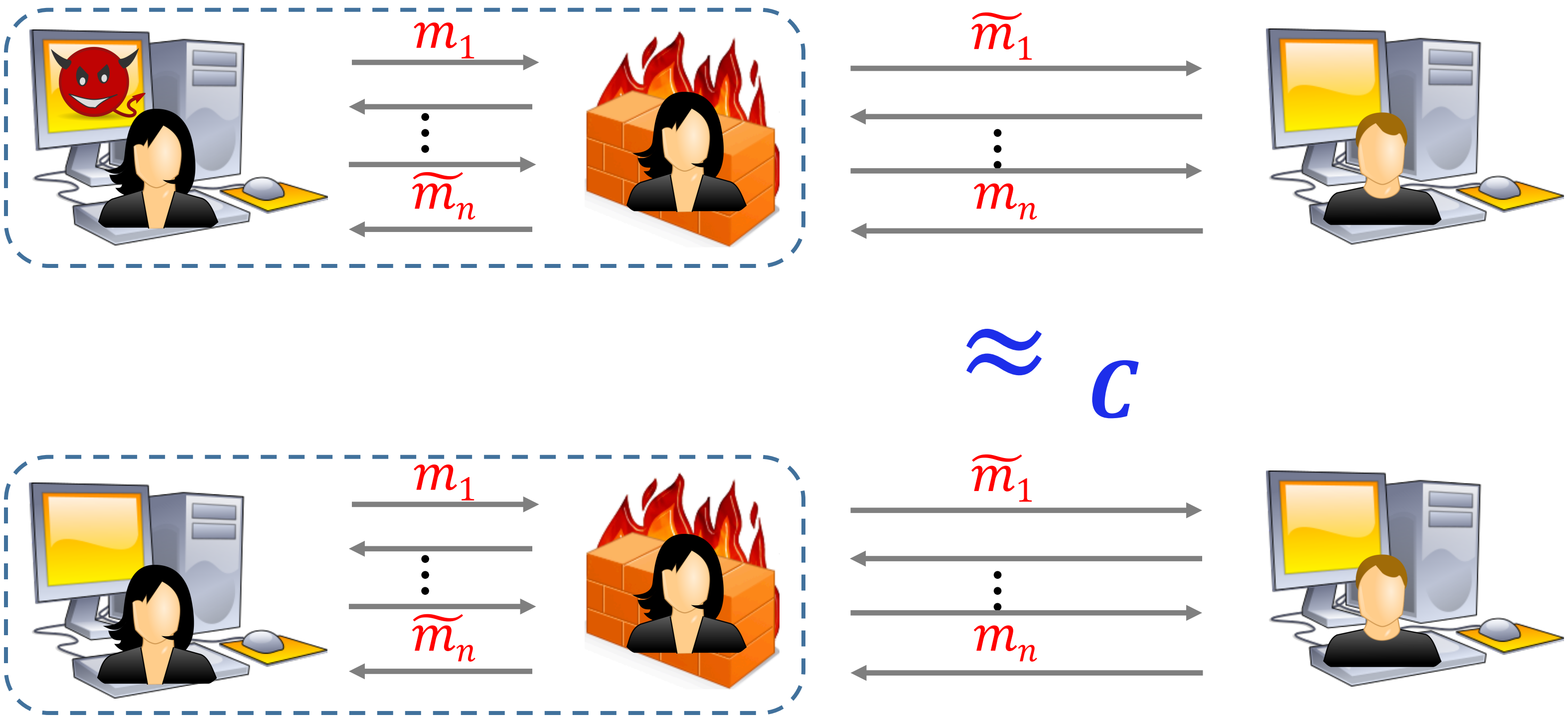
- Corrupted protocol *with $\mathcal{W}$ remains secure*



Strong vs Weak Security-Preserving
Eavesdropper vs Peer Party

Property III: Exfiltration-Resistant

- Corrupted implementation of P *cannot* leak any information to an eavesdropping attacker



Strong vs Weak Exfiltration-Resistance

Eavesdropper vs Peer Party

Research Goal

> *The "holy grail" would be a full characterization of functionalities and security properties for which reverse firewall exists.*
>
> --By **Mironov** and **Stephens-Davidowitz**
>
> **Eurocrypt 2015**

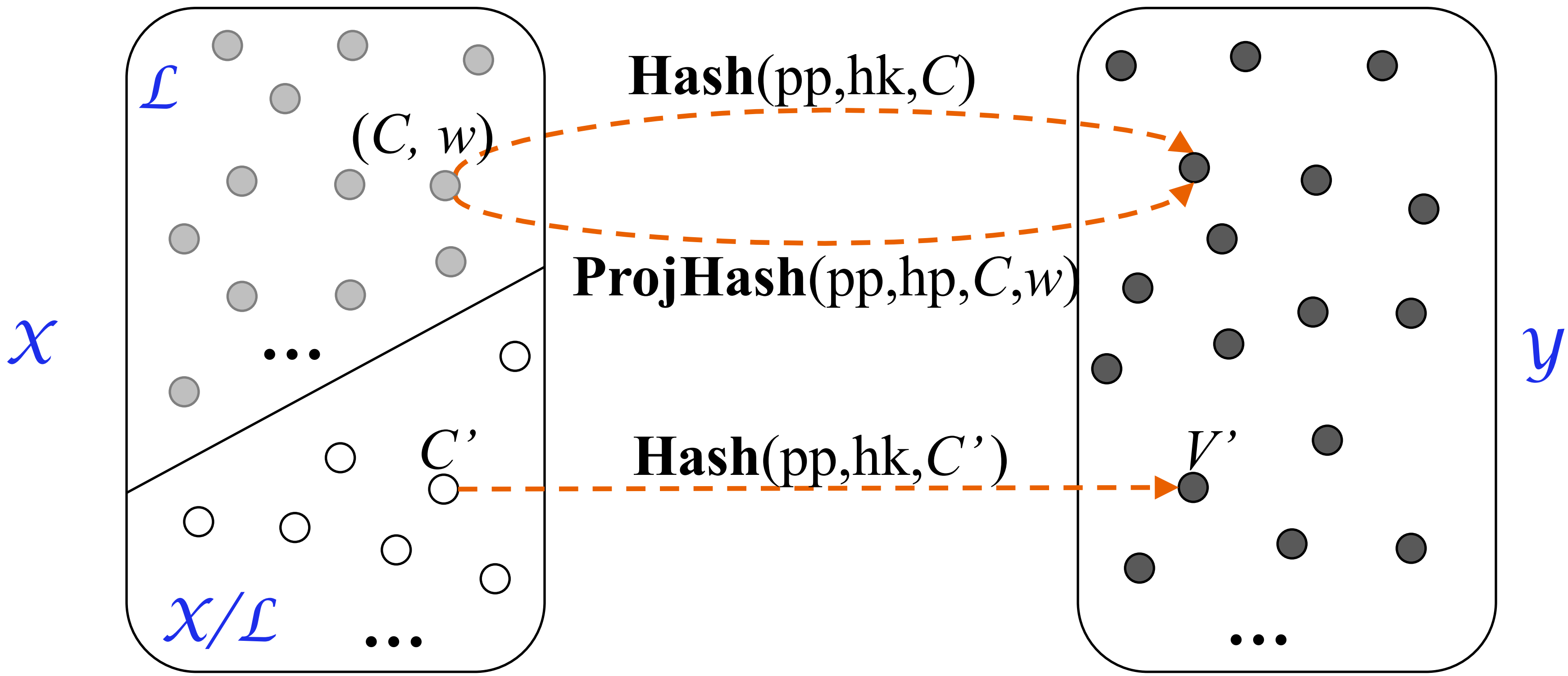
This work: a general approach for designing CRFs for functionalities that are realizable by *Smooth Projective Hash Functions*

Outline

- Background
- Cryptographic Reverse Firewall
- **Part I: Malleable Smooth Projective Hash Function**
- Part II: CRF Constructions Via Malleable SPHFs
  - Unkeyed Message Transmission Protocol
  - Oblivious Signature-Based Envelope Protocol
  - Oblivious Transfer Protocol
- Conclusions and Future Work

Smooth Projective Hash Function [CS02]

SPHFSetup(1^l)=pp; **HashKG**(pp)=hk; **ProjKG**(pp,hk)=hp



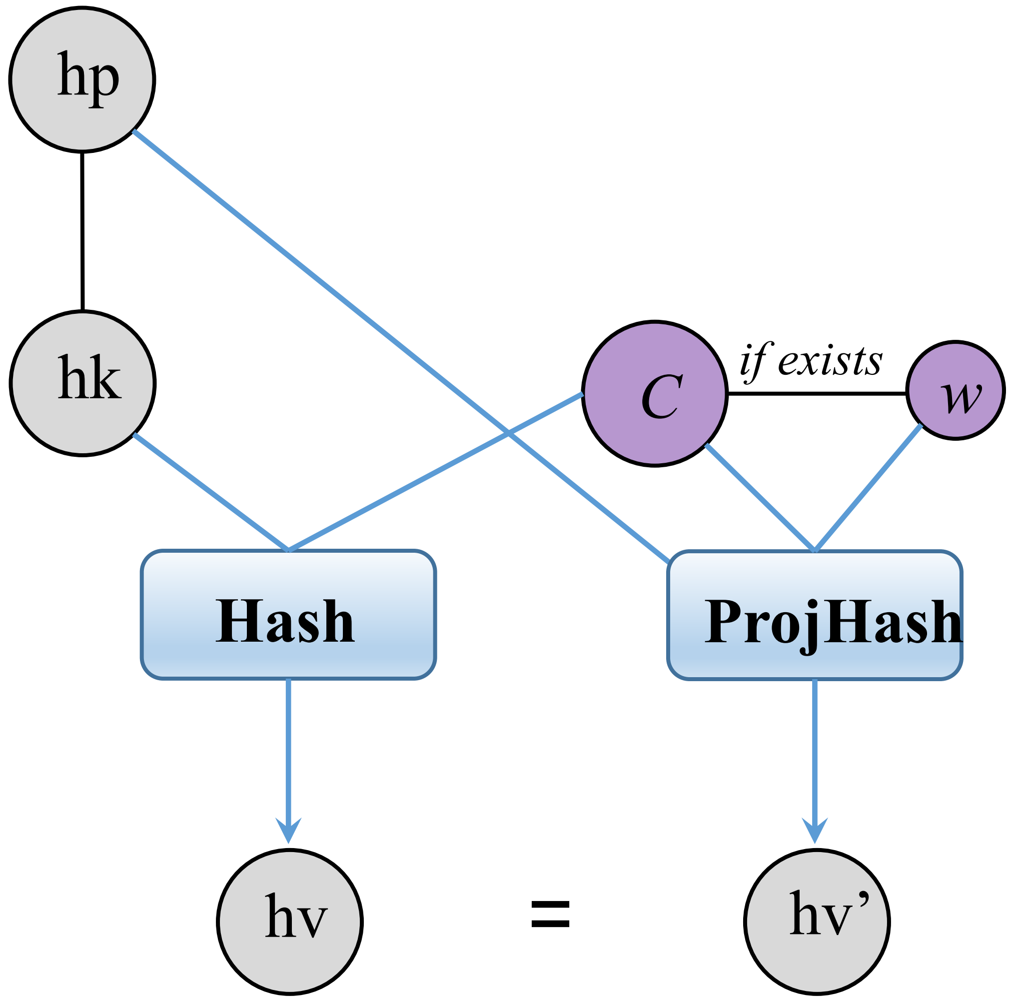
- **Correctness**: **Hash**(pp,hk,C) = **ProjHash**(pp,hp,C,w);
- **Smoothness**: $V' \approx_s R \xleftarrow{\$} \mathcal{Y}$;
- **Hard Subset Membership**: $\mathcal{L} \approx_c \mathcal{X}/\mathcal{L}$

Our Extension: Malleable SPHF

- Randomness Sampling
  - **SampR**(pp) $\longrightarrow \widetilde{r}$
  - **SampW**(pp) $\longrightarrow \widetilde{\mathrm{w}}$
- Projection Key Updating
  - **MaulK**(pp,hp, $\widetilde{r}$) $\longrightarrow \widetilde{\mathrm{hp}}$
  - **MaulH**(pp,hp, $\widetilde{r}$,C) $\longrightarrow \widetilde{\mathrm{hv}}$
- Element Re-randomization
  - **ReranE**(pp,C, $\widetilde{w}$) $\longrightarrow \widetilde{C}$
  - **ReranH**(pp,hp,C, $\widetilde{w}$) $\longrightarrow \widetilde{\mathrm{hv}}$

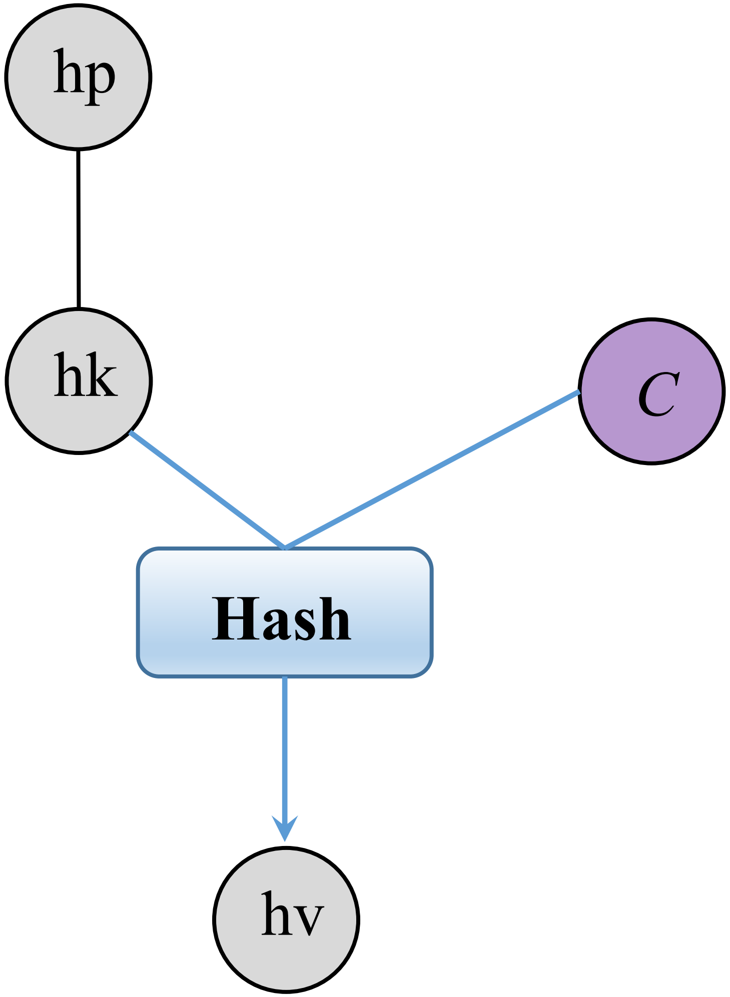
Our Extension: Malleable SPHF

- Property I: Projection Key Malleability



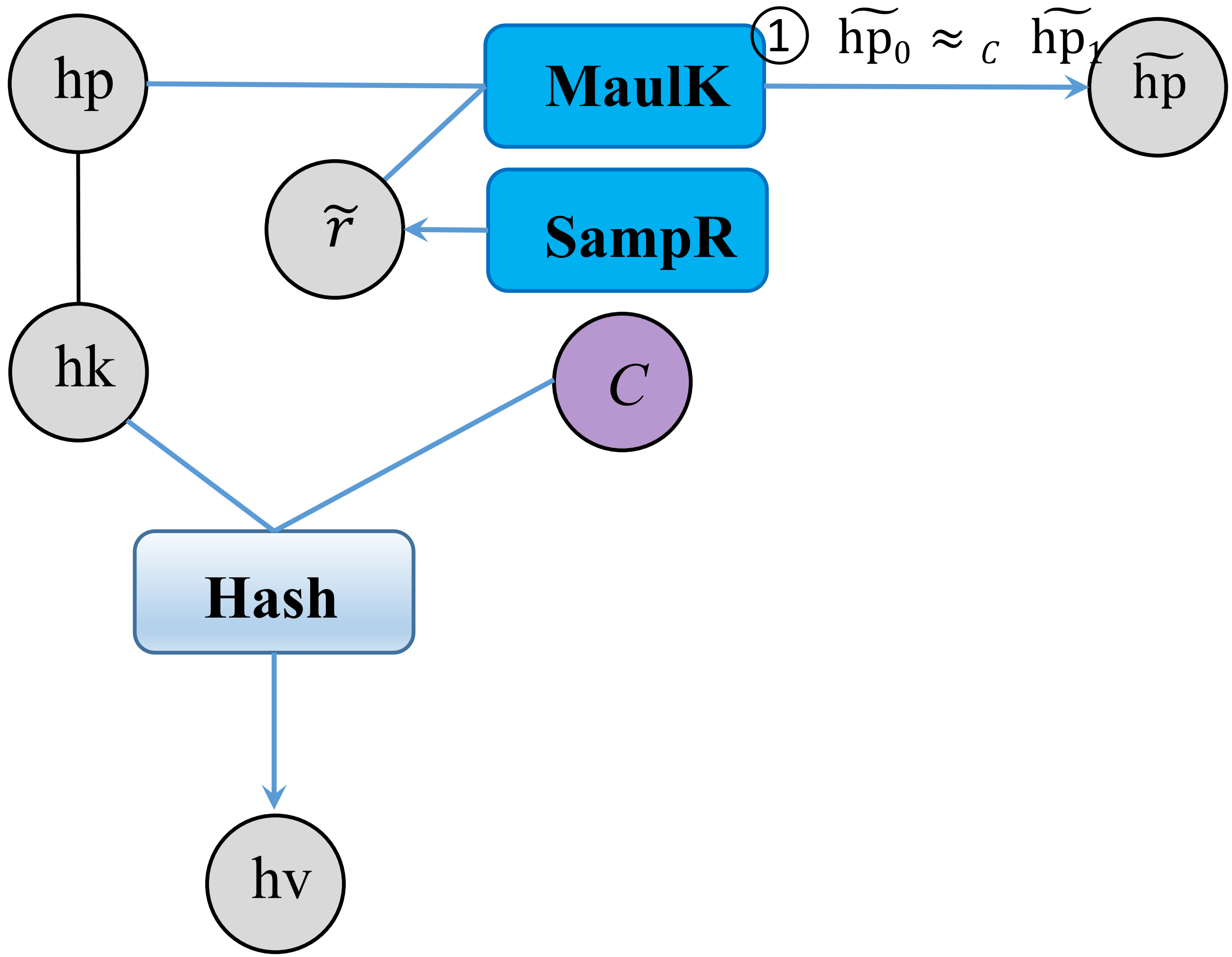
Our Extension: Malleable SPHF

- Property I: Projection Key Malleability



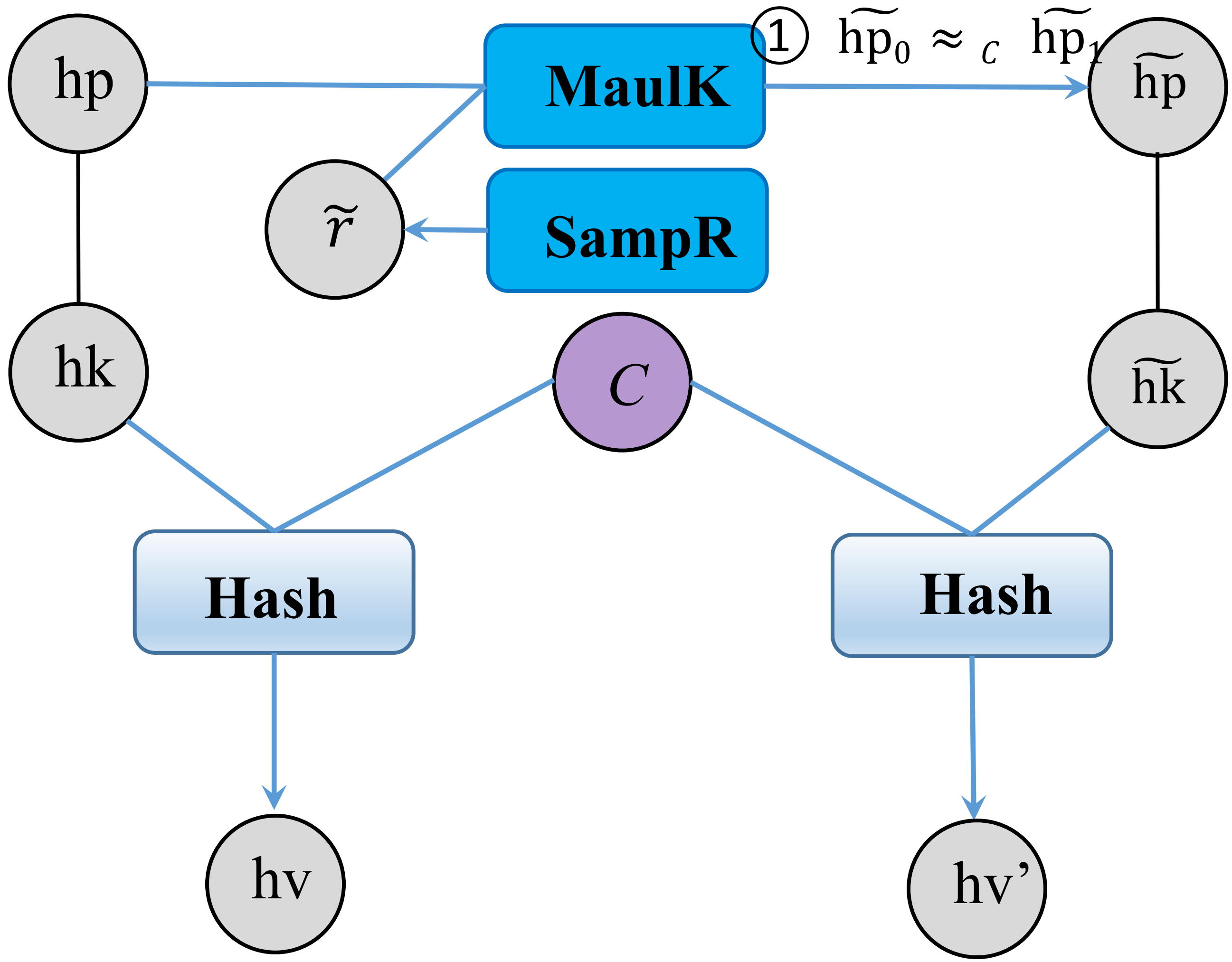
Our Extension: Malleable SPHF

- Property I: Projection Key Malleability



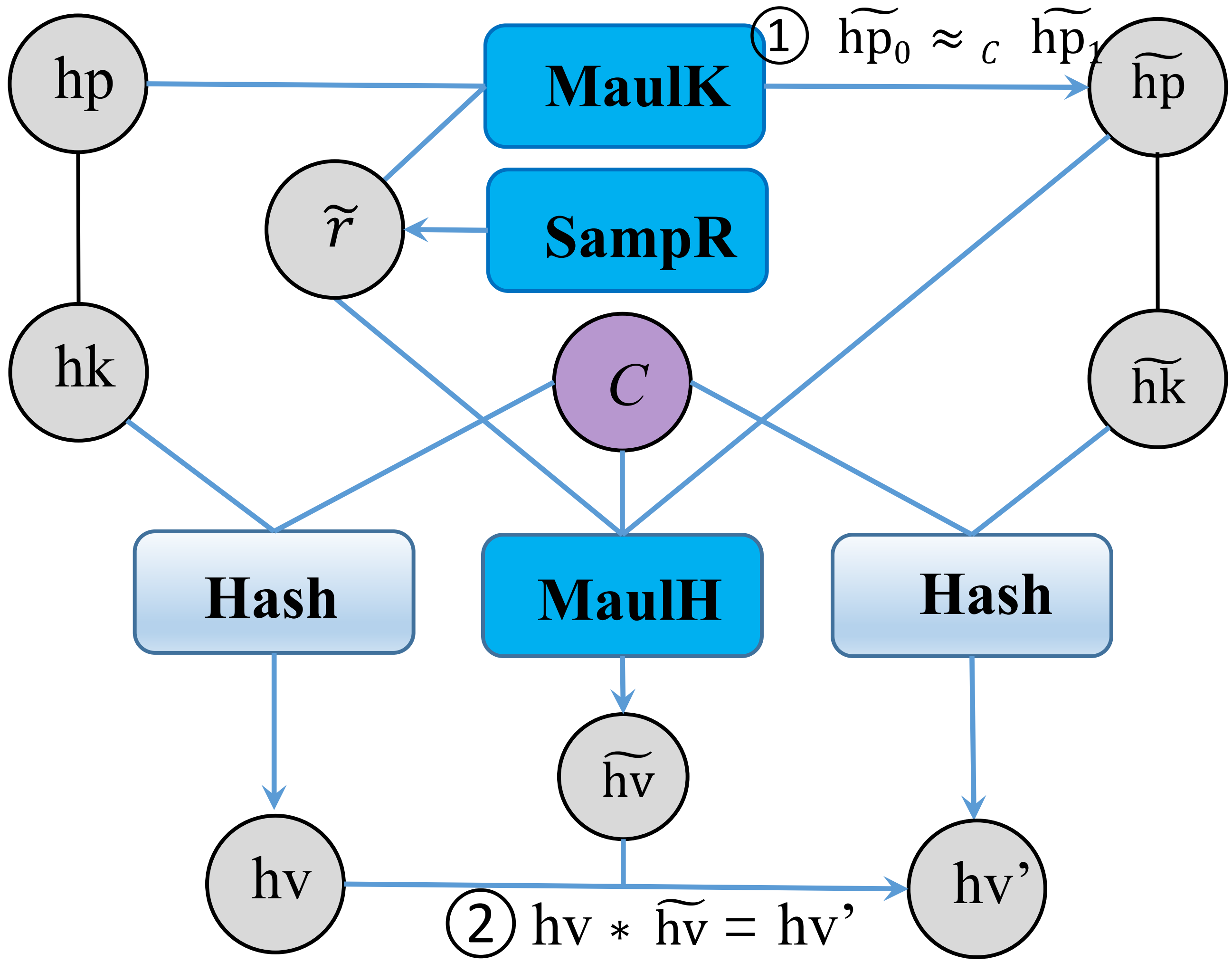
Our Extension: Malleable SPHF

- Property I: Projection Key Malleability



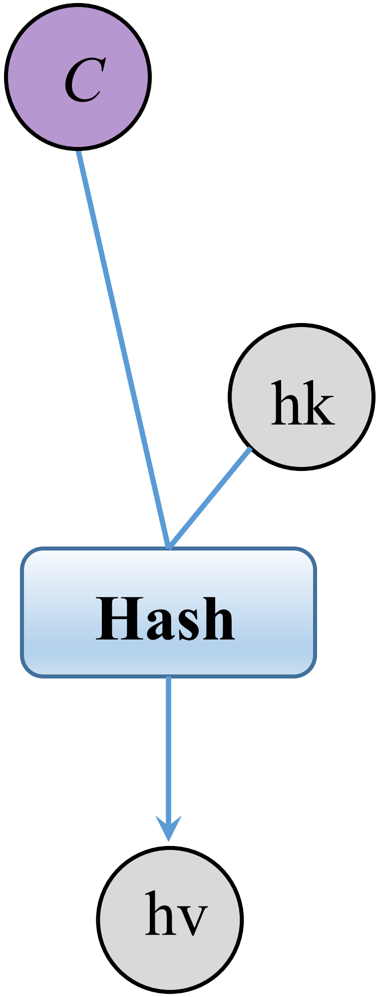
Our Extension: Malleable SPHF

- Property I: Projection Key Malleability



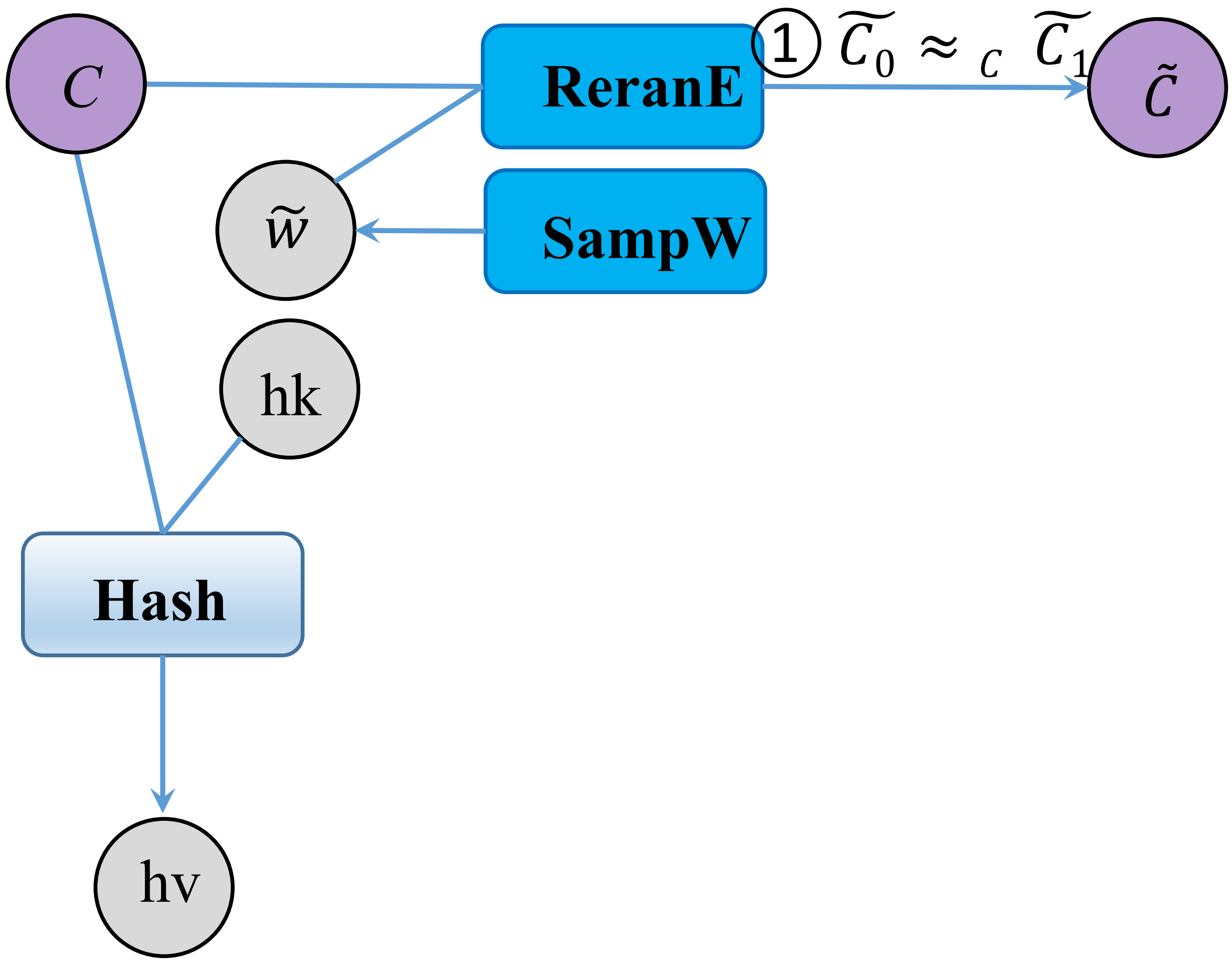
Our Extension: Malleable SPHF

- Property II: Element Re-randomizability



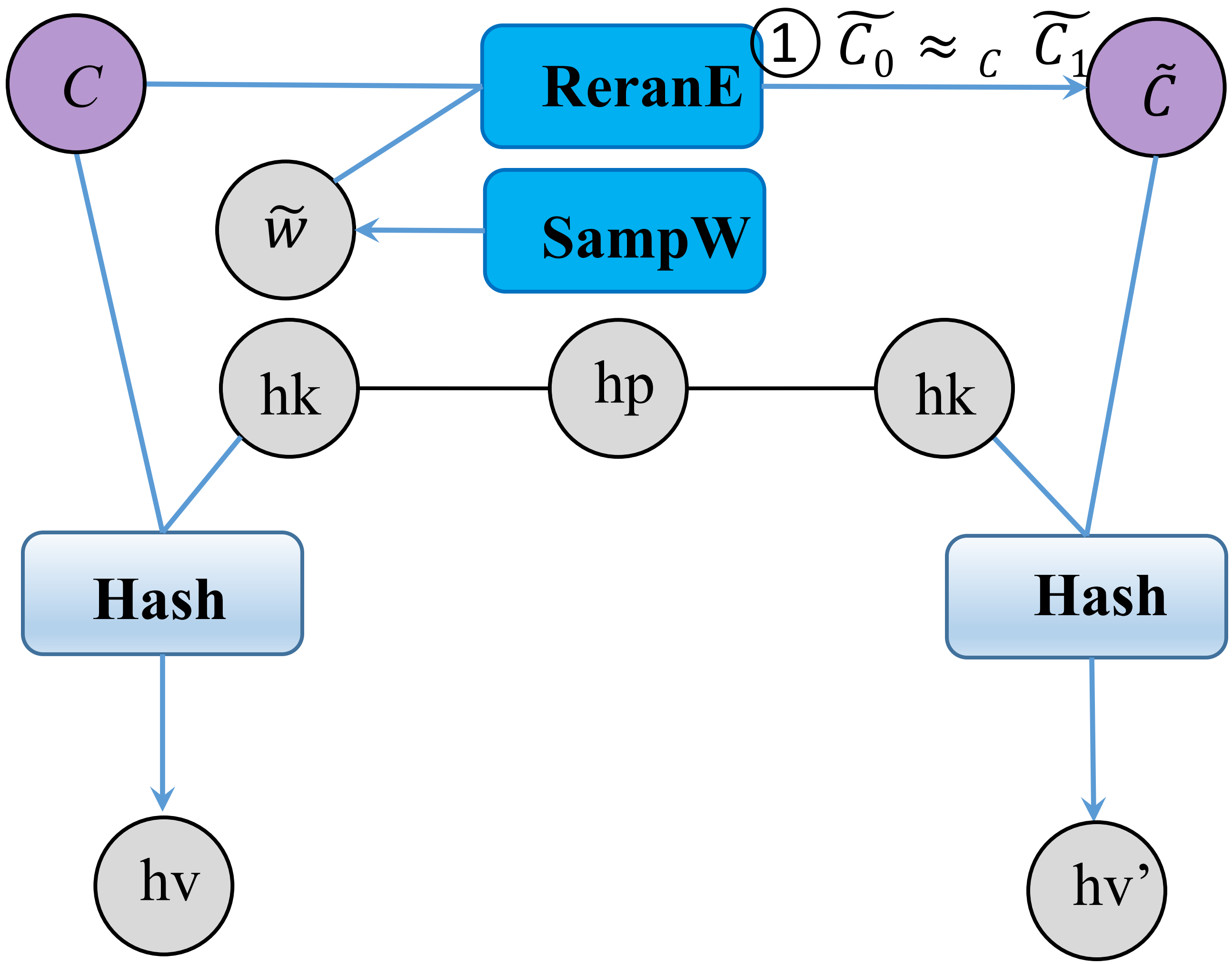
Our Extension: Malleable SPHF

- Property II: Element Re-randomizability



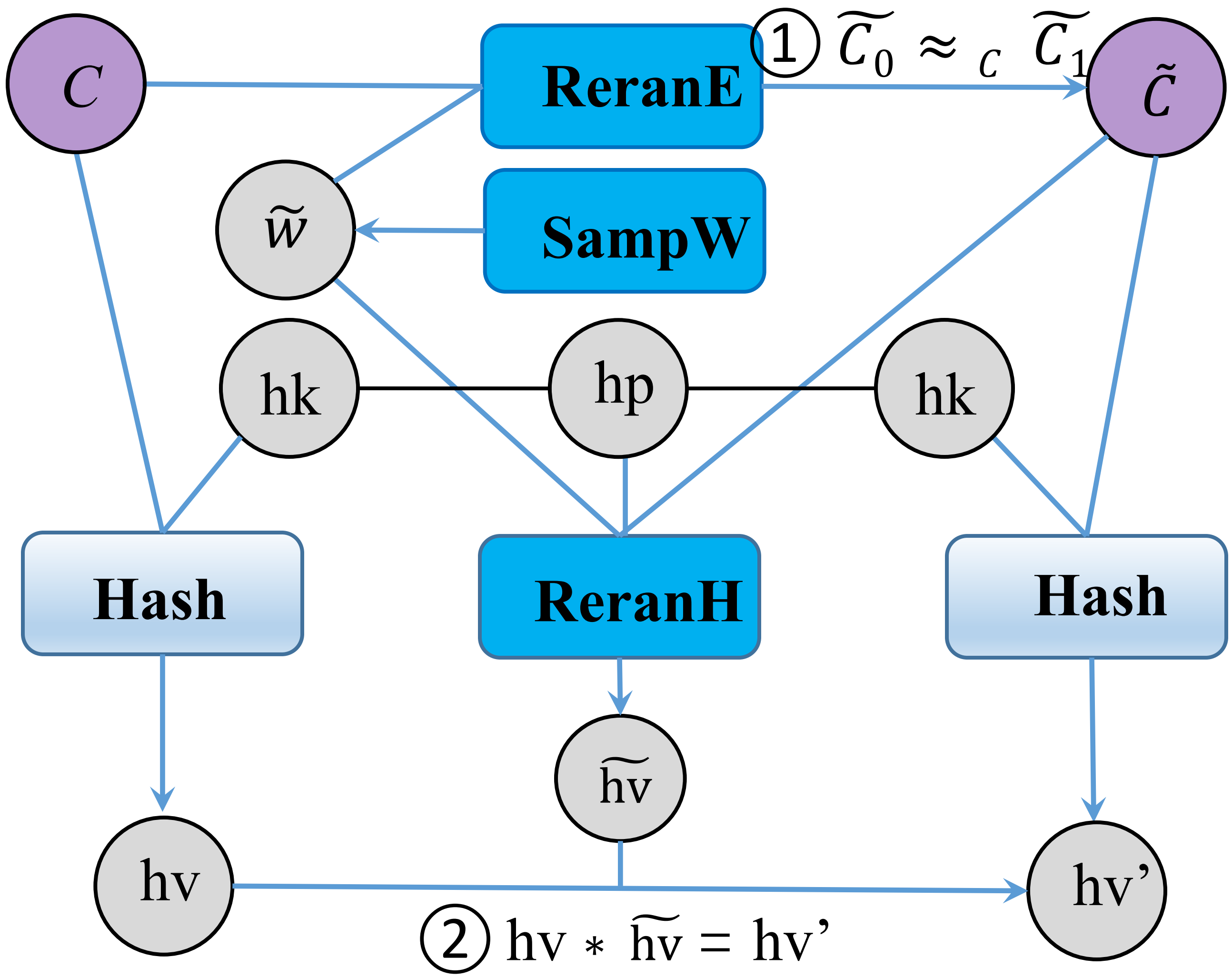
Our Extension: Malleable SPHF

- Property II: Element Re-randomizability



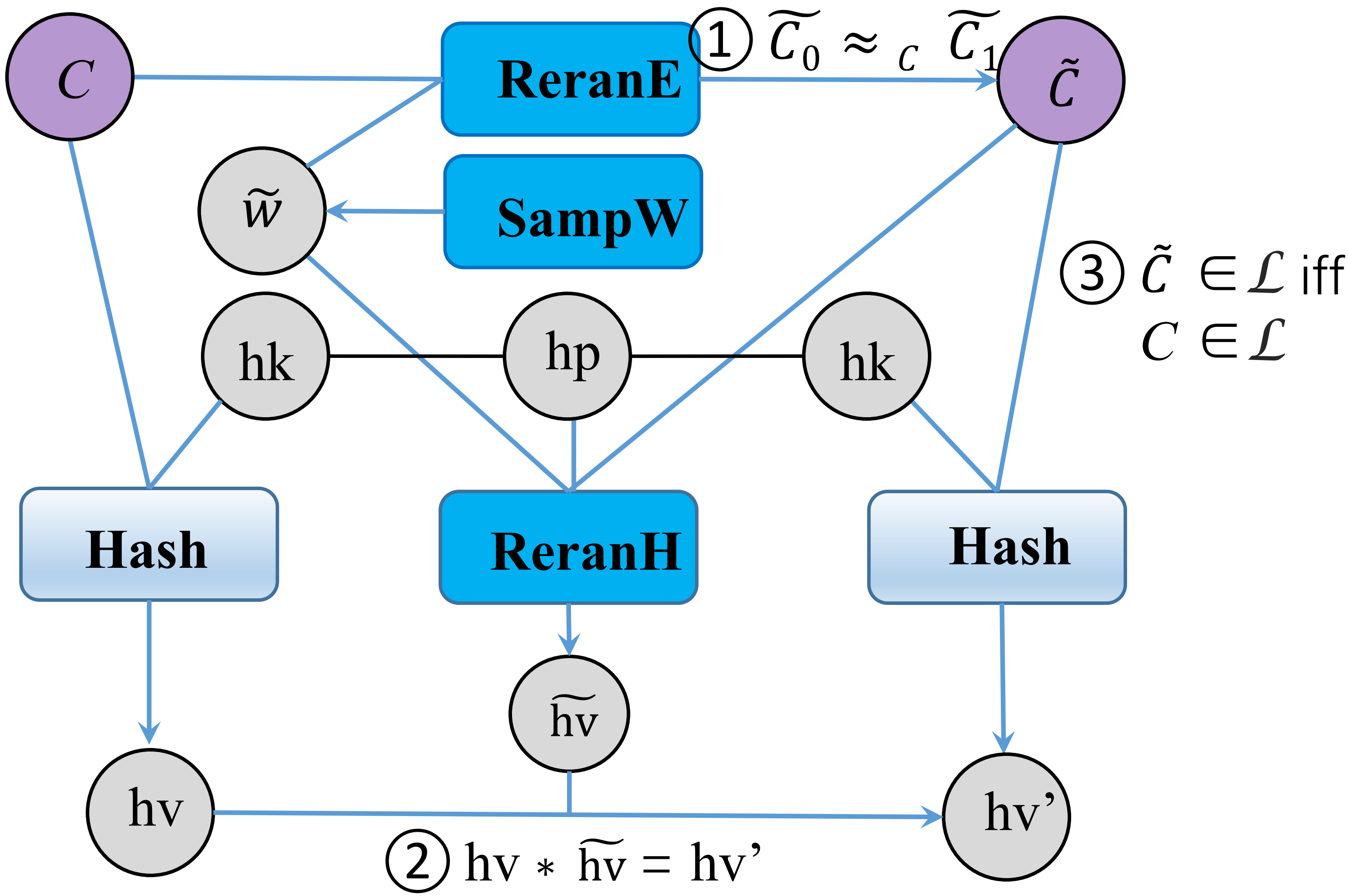
Our Extension: Malleable SPHF

- Property II: Element Re-randomizability



Our Extension: Malleable SPHF

- Property II: Element Re-randomizability



A Generic Construction of Malleable SPHF

- Graded Rings **[BCC+13]**
  - common formalization of cyclic groups, bilinear groups, and multilinear groups
  - $\forall\, a, b \in \mathbb{Z}_p,\ a \oplus b = a + b,\ a \odot b = a \cdot b$
  - $\forall\, u_1, v_1 \in \mathbb{G},\ u_1 \oplus v_1 = u_1 \cdot v_1,\ u_1 \ominus v_1 = u_1 \cdot {v_1}^{-1}$; $\forall\, c \in \mathbb{Z}_p$, $c \odot u_1 = {u_1}^c$
  - $\forall\, u_1, v_1 \in \mathbb{G}, u_1 \odot v_1 = e(u_1, v_1) \in \mathbb{G}_T$ $(e\colon \mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}_T)$
- Generic SPHF via Graded Rings **[BCC+13]**
  - $\Gamma\colon \mathcal{X} \mapsto \mathbb{G}^{m \times n}$, $\Theta\colon \mathcal{X} \mapsto \mathbb{G}^{1 \times n}$
  - $(C \in \mathcal{L}) \Leftrightarrow \left(\exists \boldsymbol{\lambda} \in {\mathbb{Z}_p}^{1 \times m} \text{ s.t.}, \Theta(C) = \boldsymbol{\lambda} \odot \Gamma(C)\right)$
  - hk$:= \boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)^{\mathrm{T}} \xleftarrow{\$} {\mathbb{Z}_p}^n$, hp $:= \gamma(C) = \Gamma(C) \odot \boldsymbol{\alpha} \in \mathbb{G}^k$
  - **Hash**(pp,hk,C) := $\Theta(C) \odot \boldsymbol{\alpha}$, **ProjHash**(pp,hp,C,w) := $\boldsymbol{\lambda} \odot \gamma(C)$

$$\Theta(C) \odot \boldsymbol{\alpha} = \boldsymbol{\lambda} \odot \Gamma(C) \odot \boldsymbol{\alpha} = \boldsymbol{\lambda} \odot \gamma(C)$$

A Generic Construction of Malleable SPHF

- Generic Malleable SPHF via Graded Rings
  - **MaulK**(pp,hp=$\gamma(C)$,$\widetilde{\boldsymbol{r}}$) : $\widetilde{\text{hp}} = \gamma(C) \oplus \Gamma(C) \odot \widetilde{\boldsymbol{r}}$
  - **MaulH**(pp,hp,$\widetilde{\boldsymbol{r}}$,$C$) : $\widetilde{\text{hv}} = \Theta(C) \odot \widetilde{\boldsymbol{r}}$
  - **ReranK**(pp,C,$\widetilde{w}$) : $\widetilde{C} = \Theta(C) \oplus \widetilde{\boldsymbol{\lambda}} \odot \Gamma(C)$
  - **ReranH**(pp,hp,C,$\widetilde{w}$) : $\widetilde{\text{hv}} = \widetilde{\boldsymbol{\lambda}} \odot \gamma(C)$

Theorem

The above construction is a *malleable* SPHF if the follows hold:

- $\Theta: \mathcal{X} \mapsto \mathbb{G}^{1\times n}$ is an identity function;
- $\Gamma: \mathcal{X} \mapsto \mathbb{G}^{m\times n}$ is a constant function;
- The hard subset membership holds.

- Instantiation from the k-linear assumption

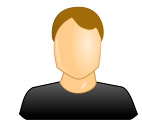
Outline

- Background
- Cryptographic Reverse Firewall
- Part I: Malleable Smooth Projective Hash Function
- **Part II: CRF Constructions Via Malleable SPHFs**
  - **Unkeyed Message Transmission Protocol**
  - Oblivious Signature-Based Envelope Protocol
  - Oblivious Transfer Protocol
- Conclusions and Future Work

Message Transmission Protocol with CRFs

- Message Transmission Protocol

Input: pp, M



Input: pp

$\text{hk} \xleftarrow{\$} \textbf{HashKG}(\text{pp})$

$\text{hp} \leftarrow \textbf{ProjKG}(\text{pp},\text{hk})$

$\xleftarrow{\quad \text{hp} \quad}$

$(C, w) \xleftarrow{\$} \textbf{SampYes}(\text{pp})$

$V = \textbf{ProjHash}(\text{pp},\text{hp},C,w)$

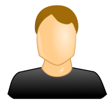
$CT = V \oplus M$

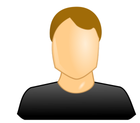
$\xrightarrow{\quad (C, CT) \quad}$

$M' = CT \ominus \textbf{Hash}(\text{pp},\text{hk},C)$

$\textbf{Hash}(\text{pp},\text{hk},C) = \textbf{ProjHash}(\text{pp},\text{hp},C,w) \Longrightarrow M' = M$

Message Transmission Protocol with CRFs

- Firewall for 



Input: pp, M | **Input:** pp | **Input:** pp

$\text{hk} \xleftarrow{\$} \textbf{HashKG}(\text{pp})$

$\text{hp} \leftarrow \textbf{ProjKG}(\text{pp},\text{hk})$

Bob's output message

$\xleftarrow{\text{hp}}$

$(C, w) \xleftarrow{\$} \textbf{SampYes}(\text{pp})$

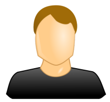
$V = \textbf{ProjHash}(\text{pp},\text{hp},C,w)$

$CT = V \oplus M$

$\xrightarrow{(C,\, CT)}$

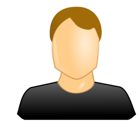
$M' = CT \ominus \textbf{Hash}(\text{pp},\text{hk},C)$

Message Transmission Protocol with CRFs

- Firewall for 

Input: pp, M

Input: pp



Input: pp

$\text{hk} \xleftarrow{\$} \textbf{HashKG}(\text{pp})$

$\text{hp} \leftarrow \textbf{ProjKG}(\text{pp},\text{hk})$

$\xleftarrow{\text{hp}}$

$\tilde{r} \xleftarrow{\$} \textbf{SampR}(\text{pp})$

$\widetilde{\text{hp}} \leftarrow \textbf{MaulK}(\text{pp},\text{hp},\tilde{r})$

$\xleftarrow{\widetilde{\text{hp}}}$

$(C, w) \xleftarrow{\$} \textbf{SampYes}(\text{pp})$

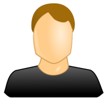
$V = \textbf{ProjHash}(\text{pp},\widetilde{\text{hp}},C,w)$

$CT = V \oplus M$

$\xrightarrow{(C,\, CT)}$

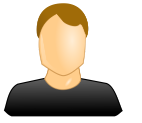
$M' = CT \ominus \textbf{Hash}(\text{pp},\text{hk},C)$

Message Transmission Protocol with CRFs

- Firewall for 

Input: pp, M

Input: pp



Input: pp

$\mathrm{hk} \overset{\$}{\leftarrow} \mathbf{HashKG}(\mathrm{pp})$

$\mathrm{hp} \leftarrow \mathbf{ProjKG}(\mathrm{pp},\mathrm{hk})$

$\xleftarrow{\mathrm{hp}}$

$\tilde{r} \overset{\$}{\leftarrow} \mathbf{SampR}(\mathrm{pp})$

$\widetilde{\mathrm{hp}} \leftarrow \mathbf{MaulK}(\mathrm{pp},\mathrm{hp},\tilde{r})$

$\xleftarrow{\widetilde{\mathrm{hp}}}$

$(C, w) \overset{\$}{\leftarrow} \mathbf{SampYes}(\mathrm{pp})$

$V = \mathbf{ProjHash}(\mathrm{pp},\widetilde{\mathrm{hp}},C,w)$

$CT = V \oplus M$

$\xrightarrow{(C,\, CT)}$

$\Delta V = \mathbf{MaulH}(\mathrm{pp},\mathrm{hp},C,\tilde{r})$

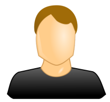
$\widetilde{CT} = CT \ominus \Delta V$

$\xrightarrow{(C,\, \widetilde{CT})}$

$M' = \widetilde{CT} \ominus \mathbf{Hash}(\mathrm{pp},\mathrm{hk},C)$

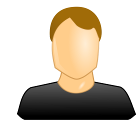
$\widetilde{CT} = CT \ominus \Delta V = V \ominus \Delta V \oplus M = \mathbf{Hash}(\mathrm{pp},\mathrm{hk},C) \oplus M \Longrightarrow M' = M$

Message Transmission Protocol with CRFs

- Firewall for 

Input: pp, M

Input: pp



Input: pp

Strong Exfiltration-Resistance

$hk \xleftarrow{\$} \textbf{HashKG}(pp)$

$hp \leftarrow \textbf{ProjKG}(pp,hk)$

$\xleftarrow{hp}$

$\tilde{r} \xleftarrow{\$} \textbf{SampR}(pp)$

$\widetilde{hp} \leftarrow \textbf{MaulK}(pp,hp,\tilde{r})$

$\xleftarrow{\widetilde{hp}}$

$(C, w) \xleftarrow{\$} \textbf{SampYes}(pp)$

$V = \textbf{ProjHash}(pp,\widetilde{hp},C,w)$

$CT = V \oplus M$

$\xrightarrow{(C, CT)}$

$\Delta V = \textbf{MaulH}(pp,hp,C,\tilde{r})$

$\widetilde{CT} = CT \ominus \Delta V$

$\xrightarrow{(C, \widetilde{CT})}$

$M' = \widetilde{CT} \ominus \textbf{Hash}(pp,hk,C)$

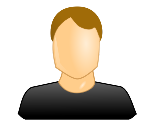
$\widetilde{CT} = CT \ominus \Delta V = V \ominus \Delta V \oplus M = \textbf{Hash}(pp,hk,C) \oplus M \Longrightarrow M' = M$

Message Transmission Protocol with CRFs

- Firewall for 

Input: pp, M

Input: pp



Input: pp

$\mathrm{hk} \overset{\$}{\leftarrow} \mathbf{HashKG}(\mathrm{pp})$

$\mathrm{hp} \leftarrow \mathbf{ProjKG}(\mathrm{pp},\mathrm{hk})$

$\xleftarrow{\mathrm{hp}}$

$(C, w) \overset{\$}{\leftarrow} \mathbf{SampYes}(\mathrm{pp})$

$V = \mathbf{ProjHash}(\mathrm{pp},\mathrm{hp},C,w)$

$CT = V \oplus M$

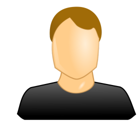
Alice's output message

$\xrightarrow{(C,\, CT)}$

$M' = CT \ominus \mathbf{Hash}(\mathrm{pp},\mathrm{hk},C)$

Message Transmission Protocol with CRFs

- Firewall for 



Input: pp, M | **Input:** pp | **Input:** pp

$\text{hk} \xleftarrow{\$} \textbf{HashKG}(\text{pp})$

$\text{hp} \leftarrow \textbf{ProjKG}(\text{pp},\text{hk})$

$\xleftarrow{\quad \text{hp} \quad}$

$(C, w) \xleftarrow{\$} \textbf{SampYes}(\text{pp})$

$V = \textbf{ProjHash}(\text{pp},\text{hp},C,w)$

$CT = V \oplus M$

$\xrightarrow{(C,\, CT)}$

$\widetilde{w} \xleftarrow{\$} \textbf{SampW}(\text{pp})$

$\widetilde{C} = \textbf{ReranE}(\text{pp},C,\widetilde{w})$

$\Delta V = \textbf{ReranH}(\text{pp},\text{hp},C,\widetilde{w})$

$\widetilde{CT} = CT \oplus \Delta V$

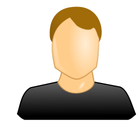
$\xrightarrow{(\widetilde{C},\, \widetilde{CT})}$

$M' = \widetilde{CT} \ominus \textbf{Hash}(\text{pp},\text{hk},\widetilde{C})$

$$\widetilde{CT} = CT \oplus \Delta V = V \oplus \Delta V \oplus M = \textbf{Hash}(\text{pp},\text{hk},\widetilde{C}) \oplus M \Longrightarrow M' = M$$

Message Transmission Protocol with CRFs

- Firewall for 

		
Input: pp, M	**Input:** pp	**Input:** pp
	Weak Exfiltration-Resistance (against Bob)	$hk \xleftarrow{\$} \mathbf{HashKG}(pp)$ $hp \leftarrow \mathbf{ProjKG}(pp,hk)$
	$\xleftarrow{\quad hp \quad}$	
$(C, w) \xleftarrow{\$} \mathbf{SampYes}(pp)$ $V = \mathbf{ProjHash}(pp,hp,C,w)$ $CT = V \oplus M$ $\xrightarrow{(C,\, CT)}$	$\widetilde{w} \xleftarrow{\$} \mathbf{SampW}(pp)$ $\widetilde{C} = \mathbf{ReranE}(pp,C,\widetilde{w})$ $\Delta V = \mathbf{ReranH}(pp,hp,C,\widetilde{w})$ $\widetilde{CT} = CT \oplus \Delta V$ $\xrightarrow{(\widetilde{C},\, \widetilde{CT})}$	$M' = \widetilde{CT} \ominus \mathbf{Hash}(pp,hk,\widetilde{C})$

$$\widetilde{CT} = CT \oplus \Delta V = V \oplus \Delta V \oplus M = \mathbf{Hash}(pp,hk,\widetilde{C}) \oplus M \Longrightarrow M' = M$$

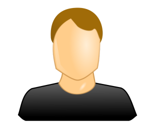
Outline

- Background
- Cryptographic Reverse Firewall
- Part I: Malleable Smooth Projective Hash Function
- **Part II: CRF Constructions Via Malleable SPHFs**
  - Unkeyed Message Transmission Protocol
  - **Oblivious Signature-Based Envelope Protocol**
  - Oblivious Transfer Protocol
- Conclusions and Future Work

Oblivious Signature-Based Envelope with CRFs

- Oblivious Signature-Based Envelope **[BPV'12]**

$\mathcal{L}$ = {valid encryption of σ_M}



Input: pp, P, M

Input: pp, σ, M

$C_\sigma \stackrel{\$}{\leftarrow}$ **Encrypt**(pp, σ; r)

$\xleftarrow{C_\sigma}$

hk $\stackrel{\$}{\leftarrow}$ **HashKG**(pp)

hp $\leftarrow$ **ProjKG**(pp,hk)

V = **Hash**(pp,hk,C_σ)

$Q = V \oplus P$

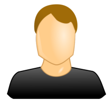
$\xrightarrow{(\text{hp}, Q)}$

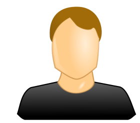
V'=**ProjHash**(pp,hp,C_σ,r)

$P' = Q \ominus V'$

$P' = P$ iff σ is a valid signature of predefined message M

Oblivious Signature-Based Envelope with CRFs

- Firewall for 



Input: pp, P, M | **Input:** pp, M | **Input:** pp, σ, M

$C_\sigma \overset{\$}{\leftarrow}$ **Encrypt**(pp, $\sigma; r$)

$\leftarrow C_\sigma$

$\widetilde{w} \overset{\$}{\leftarrow}$ **SampW**(pp)

$\widetilde{C_\sigma}$ = **ReranE**(pp, C_σ, $\widetilde{w}$)

$\leftarrow \widetilde{C_\sigma}$

hk $\overset{\$}{\leftarrow}$ **HashKG**(pp)

hp $\leftarrow$ **ProjKG**(pp,hk)

V = **Hash**(pp,hk,$\widetilde{C_\sigma}$)

$Q = V \oplus P$

(hp, Q) $\rightarrow$

ΔV = **ReranH**(pp,hp,C_σ,$\widetilde{w}$)

$\tilde{Q} = Q \ominus \Delta V$

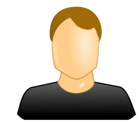
(hp, $\tilde{Q}$) $\rightarrow$

V'=**ProjHash**(pp,hp, C_σ, r)

$P' = \tilde{Q} \ominus V'$

Oblivious Signature-Based Envelope with CRFs

- Firewall for 



Input: pp, P, M

Input: pp, M

Input: pp, σ, M

$C_\sigma \overset{\$}{\leftarrow}$ **Encrypt**(pp, σ; r)

$\xleftarrow{C_\sigma}$

hk $\overset{\$}{\leftarrow}$ **HashKG**(pp)

hp $\leftarrow$ **ProjKG**(pp,hk)

V = **Hash**(pp,hk,C_σ)

$Q = V \oplus P$

$\xrightarrow{(\text{hp}, Q)}$

$\tilde{r} \overset{\$}{\leftarrow}$ **SampR**(pp)

$\widetilde{\text{hp}} \leftarrow$ **ProjMaul**(pp,hp,$\tilde{r}$)

ΔV = **MaulH**(pp,hp,C_σ,$\tilde{r}$)

$\tilde{Q} = Q \oplus \Delta V$

$\xrightarrow{(\widetilde{\text{hp}}, \tilde{Q})}$

V'=**ProjHash**(pp, $\widetilde{\text{hp}}$,C_σ,r)

$P' = \tilde{Q} \ominus V'$

Oblivious Signature-Based Envelope with CRFs

- Instantiation of OSBE **[BPV'12]**
  - Linear Encryption of Waters Signatures

$$\mathcal{L} = \Big\{(c_1, c_2, c_3, c_4) | \exists (r_1, r_2) \in \mathbb{Z}_p^2, (\sigma_1, \sigma_2) \in \mathbb{G}_1^2, \text{s.t.}, \big(c_1 = Y_1^{r_1}, c_2 = Y_2^{r_2}, c_3 = g^{r_1+r_2} \cdot \sigma_1, c_4 = \sigma_2\big) \bigwedge \big(e(g, \sigma_1) = e(\mathsf{vk}, h) \cdot e(\mathcal{F}(M), \sigma_2)\big)\Big\}.$$

- We extend the instantiation to be a malleable SPHF
  - Follow the *Graded-Ring SPFH* paradigm
  - $\Theta: \mathcal{X} \longmapsto \mathbb{G}^{1\times n}$ is not an identity function

Outline

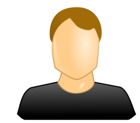
- Background
- Cryptographic Reverse Firewall
- Part I: Malleable Smooth Projective Hash Function
- **Part II: CRF Constructions Via Malleable SPHFs**
  - Unkeyed Message Transmission Protocol
  - Oblivious Signature-Based Envelope Protocol
  - **Oblivious Transfer Protocol**
- Conclusions and Future Work

Oblivious Transfer with CRFs

- OT via Graded Rings (Variant of HK-OT [HK'12])

Input: pp, M_1, M_2

Input: pp



Input: pp, b

$\boldsymbol{\Gamma} \overset{\$}{\leftarrow}$ **SampB**(pp)

$(C_b, \boldsymbol{w}) \overset{\$}{\leftarrow}$ **SampI**$(\boldsymbol{\Gamma}, b)$

$\xleftarrow{(\boldsymbol{\Gamma},\, C_b)}$

$C_{1-b} =$ **PairG**$(\boldsymbol{\Gamma}, C_b)$

$\mathrm{hk}_0 = \boldsymbol{\alpha}_0 \overset{\$}{\leftarrow} \mathbb{Z}_p{}^n$, $\mathrm{hp}_0 = \gamma_0 = \boldsymbol{\Gamma} \odot \boldsymbol{\alpha}_0$

$\mathrm{hk}_1 = \boldsymbol{\alpha}_1 \overset{\$}{\leftarrow} \mathbb{Z}_p{}^n$, $\mathrm{hp}_1 = \gamma_1 = \boldsymbol{\Gamma} \odot \boldsymbol{\alpha}_1$

$(V_i)_{i=0}^1 \leftarrow (C_i \odot \boldsymbol{\alpha}_i)_{i=0}^1$

$(CT_i)_{i=0}^1 \leftarrow (V_i \oplus M_i)_{i=0}^1$

$\xrightarrow{(\gamma_i,\, CT_i)_{i=0}^1}$

$V_b = \lambda(\boldsymbol{w}) \odot \gamma_i$

$M_b = CT_b \ominus Vb$

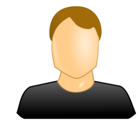
$\boldsymbol{\Gamma} = (\Gamma_1, \ldots, \Gamma_n) \in \mathbb{G}^{m \times n}$: **Element Basis**

Oblivious Transfer with CRFs

Sampl($\boldsymbol{\Gamma}, b$):	PairG($\boldsymbol{\Gamma}, C_0$):
$\boldsymbol{w} \xleftarrow{\$} \mathsf{SampW}(\mathsf{pp})$	Parse $\boldsymbol{\Gamma}$ as $(\Gamma_1, \ldots, \Gamma_n)$
$C := \lambda(\boldsymbol{w}) \odot \boldsymbol{\Gamma}$	set $\boldsymbol{\Gamma}' = (\mathbf{1}_{\mathbb{G}}, \ldots, \mathbf{1}_{\mathbb{G}}, \Gamma_n)_{1\times n}$
Parse $\boldsymbol{\Gamma}$ as $(\Gamma_1, \ldots, \Gamma_n)$	set $\boldsymbol{e} = (0_{\mathbb{Z}_p}, \ldots, 0_{\mathbb{Z}_p}, 1_{\mathbb{Z}_p})_{1\times m}$
Set $\boldsymbol{e} = (0_{\mathbb{Z}_p}, \ldots, 0_{\mathbb{Z}_p}, b_{\mathbb{Z}_p})_{1\times m}$	$\Delta C := \boldsymbol{e} \odot \boldsymbol{\Gamma}'$
$\Delta C := \boldsymbol{e} \odot (\mathbf{1}_{\mathbb{G}}, \ldots, \mathbf{1}_{\mathbb{G}}, \Gamma_n)_{1\times n}$	$C_1 := C_0 \ominus \Delta C$
$C_0 := C \oplus \Delta C$	return C_1
Return $(C_0, \boldsymbol{w})$	*Note:* $\mathbf{1}_{\mathbb{G}}$ is a $m \times 1$ matrix of $1_{\mathbb{G}}$

Oblivious Transfer with CRFs

- Firewall for 

		
Input: pp, M_1, M_2	**Input:** pp	**Input:** pp, b

Receiver:

$\boldsymbol{\Gamma} \xleftarrow{\$} \mathbf{SampB}(\mathrm{pp})$

$(C_0, \boldsymbol{w}) \xleftarrow{\$} \mathbf{SampI}(\boldsymbol{\Gamma}, b)$

$\longleftarrow (\boldsymbol{\Gamma}, c_0)$

Firewall:

$\widetilde{\boldsymbol{S}} \xleftarrow{\$} \mathbf{SampS}(\mathrm{pp})$

$\widetilde{\boldsymbol{\Gamma}} \leftarrow \boldsymbol{\Gamma} \odot \widetilde{\boldsymbol{S}}, \; C_0' \leftarrow C_0 \odot \widetilde{\boldsymbol{S}}$

$\widetilde{\boldsymbol{w}} \xleftarrow{\$} \mathbf{SampW}(\mathrm{pp})$

$C \leftarrow \lambda(\widetilde{\boldsymbol{w}}) \odot \widetilde{\boldsymbol{\Gamma}}$

$\widetilde{C_0} \leftarrow C_0' \oplus C$

$\longleftarrow (\widetilde{\boldsymbol{\Gamma}}, \widetilde{C_0})$

Sender:

$\widetilde{C_1} = \mathbf{PairG}(\widetilde{\boldsymbol{\Gamma}}, \widetilde{C_0})$

$\mathrm{hk}_0 = \boldsymbol{\alpha}_0 \xleftarrow{\$} \mathbb{Z}_p{}^n, \; \mathrm{hp}_0 = \gamma_0 = \widetilde{\boldsymbol{\Gamma}} \odot \boldsymbol{\alpha}_0$

$\mathrm{hk}_1 = \boldsymbol{\alpha}_1 \xleftarrow{\$} \mathbb{Z}_p{}^n, \; \mathrm{hp}_1 = \gamma_1 = \widetilde{\boldsymbol{\Gamma}} \odot \boldsymbol{\alpha}_1$

$(V_i)_{i=0}^1 \leftarrow (\widetilde{C}_i \odot \boldsymbol{\alpha}_i)_{i=0}^1$

$(CT_i)_{i=0}^1 \leftarrow (V_i \oplus M_i)_{i=0}^1$

$(\gamma_i, CT_i)_{i=0}^1 \longrightarrow$

Firewall:

$(\Delta V_i)_{i=0}^1 \leftarrow (\lambda(\widetilde{\boldsymbol{w}}) \odot \gamma_i)_{i=0}^1$

$(\widetilde{CT}_i)_{i=0}^1 \leftarrow (CTi \oplus \Delta Vi)_{i=0}^1$

$(\gamma_i, \widetilde{CT}_i)_{i=0}^1 \longrightarrow$

Receiver:

$V_b = \lambda(\boldsymbol{w}) \odot \gamma_i$

$M_b = \widetilde{CT}_b \ominus Vb$

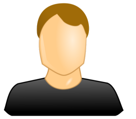
$\widetilde{\boldsymbol{S}}$: **Basis Transformation Matrix**

Oblivious Transfer with CRFs

- Firewall for 

Input: pp, M_1, M_2

Input: pp



Input: pp, b

$\boldsymbol{\Gamma} \xleftarrow{\$} \textbf{SampB}(\text{pp})$

$(C_0, \boldsymbol{w}) \xleftarrow{\$} \textbf{SampI}(\boldsymbol{\Gamma}, b)$

$\xleftarrow{(\boldsymbol{\Gamma}, C_0)}$

$C_1 = \textbf{PairG}(\boldsymbol{\Gamma}, C_0)$

$\text{hk}_0 = \boldsymbol{\alpha}_0 \xleftarrow{\$} \mathbb{Z}_p{}^n$, $\text{hp}_0 = \gamma_0 = \boldsymbol{\Gamma} \odot \boldsymbol{\alpha}_0$

$\text{hk}_1 = \boldsymbol{\alpha}_1 \xleftarrow{\$} \mathbb{Z}_p{}^n$, $\text{hp}_1 = \gamma_1 = \boldsymbol{\Gamma} \odot \boldsymbol{\alpha}_1$

$(V_i)_{i=0}^1 \leftarrow (C_i \odot \boldsymbol{\alpha}_i)_{i=0}^1$

$(CT_i)_{i=0}^1 \leftarrow (V_i \oplus M_i)_{i=0}^1$

$\xrightarrow{(\gamma_i, CT_i)_{i=0}^1}$

$\widetilde{\boldsymbol{r}_0} \xleftarrow{\$} \textbf{SampR}(\text{pp})$

$\widetilde{\boldsymbol{r}_1} \xleftarrow{\$} \textbf{SampR}(\text{pp})$

$(\widetilde{\gamma_i})_{i=0}^1 \leftarrow (\gamma_i \oplus (\boldsymbol{\Gamma} \odot \widetilde{\boldsymbol{r}_i}))_{i=0}^1$

$(\Delta V i)_{i=0}^1 \leftarrow (C_i \odot \widetilde{\boldsymbol{r}_i})_{i=0}^1$

$(\widetilde{CT}_i)_{i=0}^1 \leftarrow (CTi \oplus \Delta V i)_{i=0}^1$

$\xrightarrow{(\widetilde{\gamma_i}, \widetilde{CT}_i)_{i=0}^1}$

$V_b = \lambda(\boldsymbol{w}) \odot \widetilde{\gamma_b}$

$M_b = \widetilde{CT}_b \ominus Vb$

Instantiations of OT with CRFs

- OT-CRF construction in [MS15]

$$\boldsymbol{\Gamma} = (g, c), \quad \widetilde{\boldsymbol{S}} = \begin{pmatrix} \alpha & \alpha x' \\ 0 & \alpha \end{pmatrix}, \quad \widetilde{\boldsymbol{w}} = y',$$

$$\widetilde{\boldsymbol{\Gamma}} = \boldsymbol{\Gamma} \odot \widetilde{\boldsymbol{S}} = (g^{\alpha}, c^{\alpha} g^{\alpha x'}), \quad C_0' = C_0 \odot \widetilde{\boldsymbol{S}} = (d^{\alpha}, h^{\alpha} d^{\alpha x'}),$$

$$C = \widetilde{\boldsymbol{w}} \odot \widetilde{\boldsymbol{\Gamma}} = (g^{\alpha y'}, c^{\alpha y'} g^{\alpha x' y'}), \quad \widetilde{C_0} = C_0' \oplus C = (d^{\alpha} g^{\alpha y'}, h^{\alpha} d^{\alpha x'} c^{\alpha y'} g^{\alpha x' y'}).$$

- A more efficient variant

$$\boldsymbol{\Gamma} = (g, c) \in \mathbb{G}^{1 \times 2}, \quad \widetilde{\boldsymbol{S}} = \begin{pmatrix} s_1 & 0 \\ 0 & s_2 \end{pmatrix} \in \mathbb{Z}_p^{2 \times 2}, \quad \widetilde{\boldsymbol{w}} = y',$$

$$\widetilde{\boldsymbol{\Gamma}} = \boldsymbol{\Gamma} \odot \widetilde{\boldsymbol{S}} = (g^{s_1}, c^{s_2}), \quad C_0' = C_0 \odot \widetilde{\boldsymbol{S}} = (d^{s_1}, h^{s_2}),$$

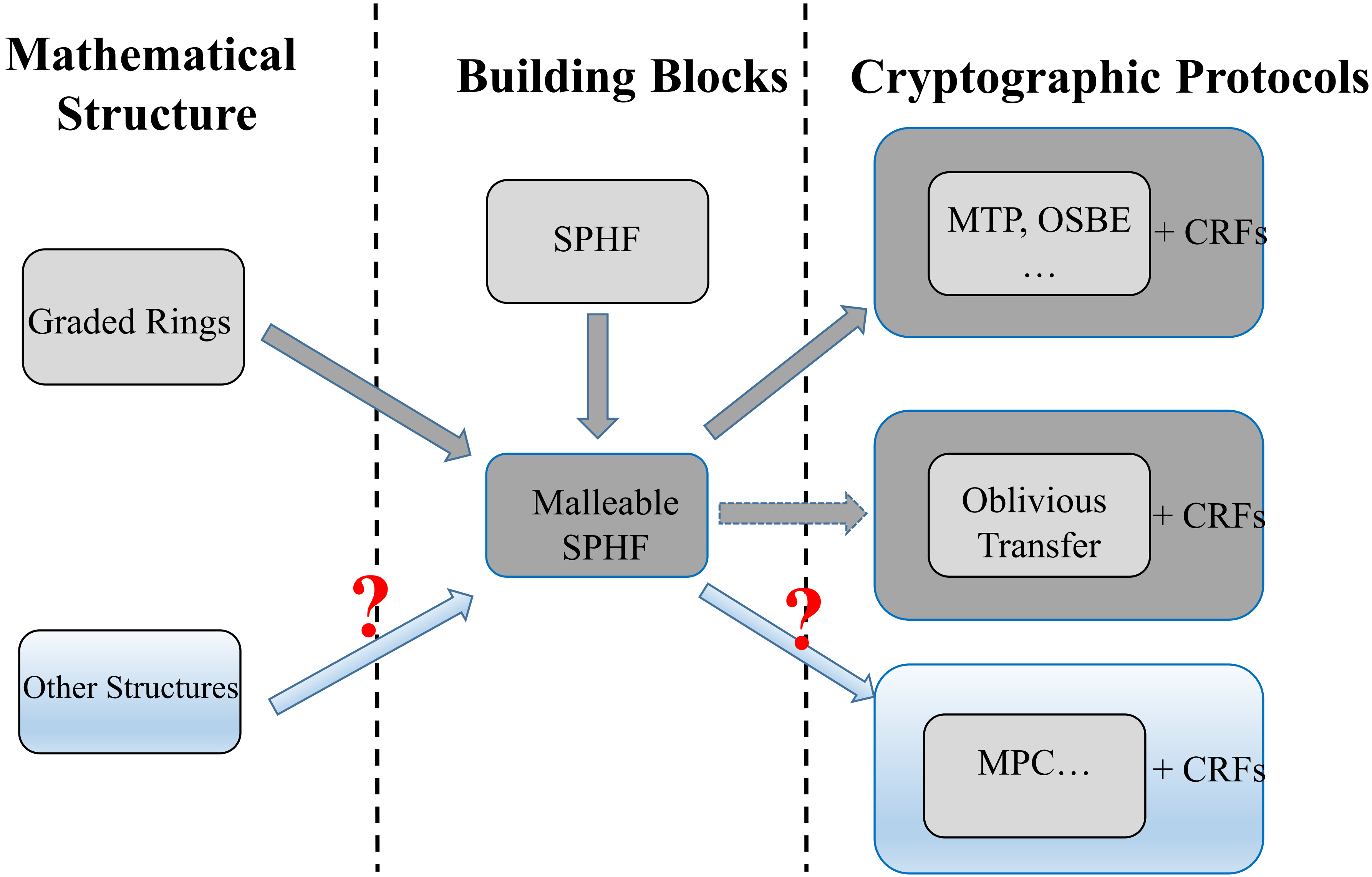
$$C = \widetilde{\boldsymbol{w}} \odot \widetilde{\boldsymbol{\Gamma}} = (g^{s_1 y'}, c^{s_2 y'}), \quad \widetilde{C_0} = C_0' \oplus C = (d^{s_1} g^{s_1 y'}, h^{s_2} c^{s_2 y'}).$$

- A more general construction based on *k*-linear assumption

Outline

- Background
- Cryptographic Reverse Firewall
- Part I: Malleable Smooth Projective Hash Function
- Part II: CRF Constructions Via Malleable SPHFs
  - Unkeyed Message Transmission Protocol
  - Oblivious Signature-Based Envelope Protocol
  - Oblivious Transfer Protocol
- **Conclusions and Future Work**

Conclusions and Future Work



Thank you ！