Policy-based Signature

Reporter:Ximeng Liu
Supervisor: Rongxing Lu

School of EEE, NTU
http://www.ntu.edu.sg/home/rxlu/seminars.htm

November 2, 2013

Main References

1. Bellare M, Fuchsbauer G. Policy-based signatures[R]. Cryptology ePrint Archive, Report 2013/413, 2013.
2. [GS08] Jens Groth, Amit Sahai. Efficient Non-interactive Proof Systems for Bilinear Groups.
3. Abe M, Fuchsbauer G, Groth J, et al. Structure-preserving signatures and commitments to group elements[M]//Advances in CryptologyCCRYPTO 2010. Springer Berlin Heidelberg, 2010: 209-236.
4. Groth J. Simulation-sound NIZK proofs for a practical language and constant size group signatures[M]//Advances in CryptologyCASIACRYPT 2006. Springer Berlin Heidelberg, 2006: 444-459.

Policy-based signature

Policy-based signatures (PBS), where a signer's secret key sk_p is associated to a policy $p \in \{0,1\}^*$ that allows the signer to produce a valid signature σ of a message m only if the message satisfies the policy, meaning (p, m) belongs to a policy language $I \subseteq \{0,1\}^* \times \{0,1\}^*$ associated to the scheme.

WHY Policy-based signature

PBS offers value along two fronts, practical and theoretical. On the practical side, the setup of PBS is natural in a corporate or other hierarchical environment. On the theoretical side, PBS decreases rather than increases complexity in the area because it serves as an umbrella notion that unies existing notions by capturing some as special cases and allows others to be derived in simple and natural ways.

Structure-preserving signature

A signature scheme is structure-preserving if its verification keys, signatures, and messages are elements in a bilinear group, and the verification equation is a conjunction of pairing-product equations.

Simulatability

Simulatability, that says that real signatures look like ones a simulator could generate without knowledge of the policy or any key derived from the policy. FE, impossibility results show that the strongest and most desirable simulation-based definitions are not achievable. PBS we will show that our simulatability notion is achievable in the standard model under standard assumptions.

Simulatability+extractability

Simulatability implies indistinguishability, and simulatability+extractability implies unforgeability.
Simulatability+extractability emerges as a powerful security notion that enables a wide range of applications.

WHAT PBS provide(1)?

Consider the example of a company implementing a scheme where each employee gets a signing key and there is one public key which is used by outsiders to verify signatures in the name of the company. A group-signature scheme would allow every employee holding a key to sign on behalf of the company, but there is no ne-grained control over who is allowed to sign which documents.

WHAT PBS provide(2)?

This can be achieved using attribute-based signatures, where each user is assigned attributes, and a message is signed with respect to a policy like (CEO or (board member and general manager)). However, it is questionable whether a verifier needs to know the company-internal policy used to sign a specific message, and there is no apparent reason he should know; all he needs to be assured of is that the message was signed by someone entitled to, but not who this person is, what she is entitled to sign, nor whether two messages were signed by the same person. This is what PBS provides.

Policy-based signature

Two generic constructions: The first uses ordinary signatures, IND-CPA encryption and standard non-interactive zero-knowledge (NIZK) proofs. Much simpler construction of PBS by relying on a more advanced cryptographic primitive: simulation-extractable (SE) NIZK proofs

Policy-based signature

Use of general NIZKs makes them inefficient⇒ Combine Groth-Sahai proofs [GS08] and structure-preserving signatures to design ecient PBS schemes for policy languages expressible via equations over a bilinear group.

Efficient Construction via Groth-Sahai Proofs

Efficient construction of PBS will be defined over a bilinear group. This is a tuple $(p, \mathbb{G}, \mathbb{H}, \mathbb{T}, G, H)$, where G, H and T are groups of prime order p, generated by G and H, respectively, and $e : \mathbb{G} \times \mathbb{H} \rightarrow \mathbb{T}$ is a bilinear map such that $e(G, H)$ generates T. We denote the group operation multiplicatively and let $1_{\mathbb{G}}$, $1_{\mathbb{H}}$ and $1_{\mathbb{T}}$ denote the neutral elements of $\mathbb{G}$, $\mathbb{H}$ and $\mathbb{T}$.

Pairing-product equation

Groth-Sahai proofs [GS08] let us prove that there exists a set of elements $(\mathbf{X}, \mathbf{Y}) = (X_1, \cdots, X_n, Y_1, \cdots, Y_l) \in \mathbb{G}^n \times \mathbb{H}^l$ which satisfy equations $E(\underline{\mathbf{X}}, \underline{\mathbf{Y}})$ of the form

$$\prod_{i=1}^{k} e(P_i, Q_i) \prod_{j=1}^{l} e(A_j, \underline{Y_j}) \prod_{i=1}^{n} e(\underline{X_i}, B_i) \prod_{i=1}^{n} \prod_{j=1}^{l} e(\underline{X_i}, \underline{Y_j})^{\gamma_{i,j}} = 1_{\mathbb{T}}$$

(1) Such an equation E is called a *pairing-product equation (PPE)* and is uniquely defined by its constants $\mathbf{P}, \mathbf{Q}, \mathbf{A}, \mathbf{B}$ $\mathbf{\Gamma} = \{\gamma_{i,j}\}_{i=[n],j=[l]}$.

Pairing-product equation

In order to hide a policy, we need to swap the roles of constants and variables in an equation, as this will enable us to hide the policy defined by the constants. We first need to transform equations as in (1) into a set of equivalent equations without exponents. To do so, we introduce auxiliary variables $\hat{Y}_{ij}$, add $i \cdot j$ new equations and define the set $E^{(no-exp)}$ as follows:

$$\prod_{i=1}^{k} e(P_i, Q_i) \prod_{j=1}^{l} e(A_j, \underline{Y_j}) \prod_{i=1}^{n} e(\underline{X_i}, B_i) \prod_{i=1}^{n} \prod_{j=1}^{l} e(\underline{X_i}, \underline{\hat{Y}_{i,j}}) = 1_{\mathbb{T}}$$

$$\wedge \bigwedge_{ij} e(G, \underline{\hat{Y}_{i,j}}) = e(G^{\gamma_{i,j}}, \underline{\hat{Y}_j}). (3)$$

A witness $(\mathbf{X}, \mathbf{Y})$ satisfies E in (2) iff $(\mathbf{X}, \mathbf{Y}, (\hat{Y}_{i,j} = Y_j^{\gamma_{ij}})_{i,j})$ satisfies the set of equations $E^{(no-exp)}$ in (3).

Pairing-product equation

we can show that a (clear) message $(\mathbf{M}, \mathbf{N})$ satisfies a "hidden" policy defined by equation E, witnessed by elements $(\mathbf{V}, \mathbf{W})$, since we can express policies as sets of group elements.

Policy checkers for PPEs.

Consider a policy p describing (for simplicity) a single equation defined by $p = (\mathbf{P}, \mathbf{Q}, \mathbf{A}, \mathbf{B}, \mathbf{K}, \mathbf{L}, \Gamma = \gamma_{i,j}, \Delta = \delta_{i,j}, \Phi = \phi_{i,j}, \Psi = \psi_{i,j})$ Let $m = (\mathbf{M}, \mathbf{N}) \in \mathbb{G}^{n^m} \times \mathbb{H}^{l_m}$ be a message $\omega = (\mathbf{V}, \mathbf{W}) \in \mathbb{G}^{n^\omega} \times \mathbb{H}^{l_\omega}$ be a witness. Then the policy checker PC for our construction is defined as follows:

$$PC((p, m), \omega) \Leftrightarrow$$

$$\prod e(P_i, Q_i) \prod e(A_j, N_j) \prod e(M_i, B_i) \prod e(K_j, W_j) \prod e(V_i, L_i)$$

$$\prod \prod e(M_i, N_j)^{\gamma_{i,j}} \prod \prod e(M_i, W_j)^{\delta_{i,j}} \prod \prod e(V_i, N_j)^{\phi_{i,j}} \prod \prod e(V_i, W_j)^{\psi_{i,j}} = 1_{\mathbb{T}}$$

Policy checkers for PPEs.

which is the most general form of a PPE over variables **M,N,V,W**. **Assume that all policies are of a fixed length**, since we cannot hide the form of the set of equations they define.

Policy checkers for PPEs.

We start with expressing a policy in terms of group elements only. Abusing notation slightly, we replace the matrices $\Gamma = \gamma_{i,j}, \Delta = \delta_{i,j}, \Phi = \phi_{i,j}, \Psi = \psi_{i,j} \in \mathbb{Z}_p^{n \times l}$ in the policy description by matrices of $\mathbb{G}$-elements$\mathbf{\Gamma} = (\Gamma_{i,j} := G^{\gamma_{i,j}})$, $\mathbf{\Delta} = (\Delta_{i,j} := G^{\delta_{i,j}})$, $\mathbf{\Phi} = (\Phi_{i,j} := G^{\phi_{i,j}})$, $\mathbf{\Psi} = (\Psi_{i,j} := G^{\psi_{i,j}})$. Applying the transformation $E \rightarrow E^{(no-exp)}$ from Equation $PC^{no-exp}((\underline{p}, m), \omega) \Leftrightarrow$

$$\prod e(\underline{P_i}, \underline{Q_i}) \prod e(\underline{A_j}, N_j) \prod e(M_i, \underline{B_i}) \prod e(\underline{K_j}, \underline{W_j}) \prod e(\underline{V_i}, \underline{L_i})$$

$$\prod \prod e(M_i, \underline{\hat{N}_{ij}^{(1)}}) \prod \prod e(M_i, \underline{\hat{W}_{ij}^{(1)}})^{\delta_{i,j}} \prod \prod e(\underline{V_i}, \underline{\hat{N}_{ij}^{(1)}}) \prod \prod e(V_i, \underline{\hat{W}_{ij}^{(1)}}) = 1_{\mathbb{T}}$$

$$\wedge \bigwedge_{i,j} e(G, \underline{\hat{N}_{ij}^{(1)}}) = e(G^{\gamma_{i,j}}, \underline{N_{ij}}) \wedge \bigwedge_{i,j} e(G, \underline{\hat{W}_{ij}^{(1)}}) = e(G^{\delta_{i,j}}, \underline{W_{ij}})$$

Policy checkers for PPEs

$$\wedge \bigwedge_{i,j} e(G, \underline{\hat{N}_{ij}^{(2)}}) = e(G^{\phi_{i,j}}, \underline{N_{ij}}) \wedge \bigwedge_{i,j} e(G, \underline{\hat{W}_{ij}^{(2)}}) = e(G^{\psi_{i,j}}, \underline{W_{ij}})$$

where we introduced new variables $\hat{N}_{ij}^{(1)}, \hat{N}_{ij}^{(2)}, \hat{W}_{ij}^{(1)}, \hat{W}_{ij}^{(2)}$ and corresponding equations. Note that these equations contain the elements from $\mathbf{\Gamma}, \mathbf{\Delta}, \mathbf{\Phi}, \mathbf{\Psi}$ as variables.

Policy checkers for PPEs

$$PC^{no-exp}((\underline{p}, m), \omega)(T) \Leftrightarrow$$

$$\prod e(\underline{P_i}, \underline{Q_i}) \prod e(\underline{A_j}, N_j i) \prod e(M_i, \underline{B_i}) \prod e(\underline{K_j}, \underline{W_j}) \prod e(\underline{V_i}, \underline{L_i})$$

$$\prod \prod e(M_i, \underline{\hat{N}_{ij}^{(1)}}) \prod \prod e(M_i, \underline{\hat{W}_{ij}^{(1)}})^{\delta_{i,j}} \prod \prod e(\underline{V_i}, \underline{\hat{N}_{ij}^{(1)}}) \prod \prod e(V_i, \underline{\hat{W}_{ij}^{(1)}}) = 1_{\mathbb{T}}$$

$$\wedge \bigwedge_{i,j} e(T, \underline{\hat{N}_{ij}^{(1)}}) = e(\Gamma_{i,j}, \underline{N_{ij}}) \wedge \bigwedge_{i,j} e(T, \underline{\hat{W}_{ij}^{(1)}}) = e(\Delta_{i,j}, \underline{W_{ij}})$$

$$\wedge \bigwedge_{i,j} e(T, \underline{\hat{N}_{ij}^{(2)}}) = e(\Phi_{i,j}, \underline{N_{ij}}) \wedge \bigwedge_{i,j} e(T, \underline{\hat{W}_{ij}^{(2)}}) = e(\Psi_{i,j}, \underline{W_{ij}})$$

Policy checkers for PPEs

$$E^{(disj)}(mvk, \underline{p}, \underline{S_1}, \underline{S_2}, \underline{\omega}, ovk, \underline{T_1}, \underline{T_2}) :$$

$$e(\underline{T_1} \cdot \underline{T_2} \cdot G^{-1}, H) = 1 \wedge$$

$$V^{(Sim)}(mvk, (G, \underline{\mathbf{P}}, \underline{\mathbf{Q}}, \underline{\mathbf{A}}, \underline{\mathbf{B}}, \underline{\mathbf{K}}, \underline{\mathbf{L}}, \underline{\mathbf{\Gamma}}, \underline{\mathbf{\Delta}}, \underline{\mathbf{\Phi}}, \underline{\mathbf{\Psi}}, \underline{S_1}))(\underline{T_1}) = 1 \wedge$$

$$PC^{(Sim)}((\underline{\mathbf{P}}, \underline{\mathbf{Q}}, \underline{\mathbf{A}}, \underline{\mathbf{B}}, \underline{\mathbf{K}}, \underline{\mathbf{L}}, \underline{\mathbf{\Gamma}}, \underline{\mathbf{\Delta}}, \underline{\mathbf{\Phi}}, \underline{\mathbf{\Psi}},), (\mathbf{M}, \mathbf{N}), (\mathbf{V}, \mathbf{W}))(\underline{T_1}) = 1 \wedge$$

$$V^{(sim)}(mvk, (1, ovk), \underline{S_2})(\underline{T_2}) = 1$$

Thank you

Rongxing's Homepage:
http://www.ntu.edu.sg/home/rxlu/index.htm
PPT available @: http://www.ntu.edu.sg/home/rxlu/seminars.htm

Ximeng's Homepage:
http://www.liuximeng.cn/